

مركز حازم لترجمة الدراسات الاستراتيجية

CYBER SECURITY

صعود الحرب الإلكترونية

الهوية والمعلومات وخصائص الحرب الحديثة

Glenn J. Voelz



صعود الحرب الإلكترونية:

الهوية والمعلومات وخصائص الحرب الحديثة

صعود الحرب الإلكترونية:

الهوية والمعلومات وخصائص الحرب الحديثة

جلين جيه. فويلز.

دراسة صادرة عن كلية حرب الجيش الأمريكي

معهد الدراسات الاستراتيجية

أكتوبر (تشرين أول) ٢٠١٥

تحت عنوان

THE RISE OF IWAR:

IDENTITY, INFORMATION, AND THE INDIVIDUALIZATION OF MODERN WARFARE

www.hazeminstitute.com

E-mail: hazeminstitute@gmail.com

ترجمة صادرة عن مركز حازم لترجمة الدراسات الاستراتيجية

صدرت الترجمة مارس (آذار) ٢٠١٨

عدد الصفحات: ١٨٧

كلما أردت مهاجمة جيش، محاصرة مدينة، أو قتل شخص ما، يجب عليك أولا معرفة هويات كبار ضباط جهاز الدفاع، أعوانهم، زائريهم، حراسهم، والقائمين على سلامتهم...

سون تزو، فن الحرب

المحتوى


حازم

كلية حرب جيش الولايات المتحدة الأمريكية

تقوم كلية **حرب جيش الولايات المتحدة الأمريكية** بتثقيف وتطوير القادة لتمكينهم من الخدمة على المستوى الاستراتيجي، وذلك بالتزامن مع تحسين معرفتهم بالتطبيقات العالمية للقوة العسكرية.

حيث يعتبر أهم أهداف كلية حرب الجيش الأمريكي؛ إعداد خريجين يتمتعون بالمهارة في التحليل النقديّ والقدرة على حل المشكلات المعقدة، وفي الوقت نفسه فإنَّه من أسمى مهامنا في جيش الولايات المتحدة الأمريكية أن نكون مَصْنَعًا للأفكار، التي يتم تقديمها للقادة العسكريين والقيادات المدنية على المستوى الاستراتيجي الدوليّ، وأن ننخرط بشكل دوريٍّ في النقاشات المستمرة، بخصوص دور القوات البرية في تحقيق أهداف الأمن القوميّ وحمايتها.



معهد الدراسات الاستراتيجية يقوم بنشر تحاليل متخصصة في البحث الاستراتيجي ودراسات الأمن القوميّ، وذلك لتقديم المعلومات اللازمة في عمليات مناقشة وإعداد السياسات العامة، ويقوم المعهد بدوره في سدِّ الفجوة بين الدراسات الأكاديمية النظرية من جهة، وبين العمل العسكريّ الفعليّ من جِهة أخرى.



مركزُ القيادة الاستراتيجية والتطوير يُسهِم في تثقيف القيادات العليا التي تعمل على مستويات عالمية، وفي دعْم المعرفة اللازمة لدى الخبراء وتحسين مستوياتهم، وتقديم الحلول لمشكلات الجيش الاستراتيجية؛ التي تؤثر بدورها على الأمن القوميّ ككل.



معهد عمليات حفظ السلام والاستقرار يقدم الخبرة اللازمة لمختلف الشؤون المتعلقة لحفظ السلام والاستقرار، ويقوم كذلك بإعداد تقارير المراجعة الفنية المتخصصة، وتقديم التقارير الكتابية المعرفية للهيئات، التي تعمل على تطوير مبادئ وأساسيات عمليات الاستقرار.



برنامج تطوير ودعم القيادات العليا يقوم بتدعيم الأقسام العسكرية المختلفة داخل كلية حرب الجيش الأمريكي؛ وذلك لتثقيف القادة الاستراتيجيين وتقديم أعلى مستويات المعرفة والتعليم لتطوير الوعي الذاتيّ لدى القيادات، من خلال تحفيزهم لتقديم آرائهم واستجاباتهم للقضايا المطروحة.



مدرسة القوة العسكرية الاستراتيجية تعمل على تطوير القادة الاستراتيجيين؛ من خلال تقديم الأساس المعرفيّ المتكامل للوصول إلى البراعة المهنية اللازمة في العمل العسكريّ للجيش، وهي المدرسة العسكرية التي تقدِّم خَدَماتها المتكاملة لتكون بَوْتقةً لتثقيف قادة المستقبل؛ للتمكن التام من عمليات تحليل وتقييم وصقل الخبرات المهنية العسكرية في مجال: الحروب، الاستراتيجيات، العمليات، الأمن القوميّ، إدارة الموارد، القيادة المسؤولة.



مركز الجيش الأمريكي للتعليم والتراث المعرفيّ، يتخصَّص في تجميع وحِفظ وعرض المواد التاريخية؛ لاستخدامها في دعْم جيش الولايات المتحدة الأمريكية، وتثقيف أفراده على المستوى العالميّ، وكذلك تكريم الجنود السابقين والحاليِّين

.

معهد الدراسات الاستراتيجية

يُعدُّ **معهد الدراسات الاستراتيجية** (إس إس آي **SSI**) جزءًا من كلية حرب الجيش الأمريكي، وهو الجهة المسؤولة عن إعداد الدراسات على المستوى الاستراتيجي للقضايا المتعلقة بالأمن القومي، والاستراتيجيات العسكرية، مع التركيز المتخصص على دراسات التحليل الاستراتيجية–الجغرافية (الدراسات الجيو–استراتيجية).

كما تعتبر مهمة **معهد الدراسات الاستراتيجية** هي تقديم التحليل المستقل؛ لإجراء الدراسات الاستراتيجية وتطوير التوصيات المتعلقة بالسياسات العسكرية، التي تَدُور بشكل رئيس حوْل العناصر التالية:

- إعداد الاستراتيجيات والخطط، والسياسات للتعيين المشترك والمجمّع لموظفي القوات العسكرية.
- إعداد التقييمات الاستراتيجية الإقليمية.
- الدراسات المتعلقة بطبيعة الحروب البرية.
- القضايا التي تؤثر على مستقبل الجيش.
- المبادئ، الفلسفة، والنظريات الاستراتيجية.
- القضايا الأخرى ذات الأهمية فيما يتعلّق بقيادة الجيش.

يتم إعداد الدراسات بواسطة المحللين المدنيين والعسكريين أيضًا فيما يخصُّ القضايا ذات التأثيرات الاستراتيجية على الجيش، ووزارة الدفاع، ومختلف المؤسسات المعنية بقضايا الأمن القوميِّ.

بالإضافة إلى الدراسات التي يقوم المعهد بإعدادها والموضحة أعلاه، فإن **معهد الدراسات الاستراتيجية** يقوم بنشر التقارير المتخصصة في القضايا الهامة ذات الطبيعة الخاصة أو العاجلة، بما في ذلك تفاصيل الاجتماعات والجلسات المعنية بمناقشة القضايا الاستراتيجية، وتقارير البعثات العسكرية الموسَّعة، وكذلك القرارات ذات الاستجابة السريعة التي قامت القيادات العليا للجيش باتخاذها.

ويعمل المعهد على دعم القدرات التحليلية المؤثرة داخل الجيش؛ لمناقشة وحل القضايا الاستراتيجية وغيرها من الأمور التي تَدعَم مساهمة الجيش الأساسية في إعداد سياسات الأمن القوميِّ.



تنبيه

الآراء الواردة في هذا التقرير هي آراء الكاتب ولا تعكس بالضرورة السياسة الرسمية أو موقف إدارة الجيش: وزارة الدفاع، أو حكومة الولايات المتحدة الأمريكية، أصدر مؤلفوا معهد الدراسات الاستراتيجية (SSI) وكلية حرب الجيش الأمريكي (USAWC) منشورات تتمتع بالحرية الأكاديمية الكاملة، وذلك بشرط عدم الإفصاح عن المعلومات السرية، وألَّا تُشكِّل تهديدًا لسلامة العمليات الجارية، وألا تقوم بتحريف السياسات الرسمية الأمريكية، هذه الحرية الأكاديمية تمكِّنهم من تقديم وجهات النظر الجديدة، التي يمكن أن تكون مثيرة للجدل في بعض الأحيان، إلا أنها دائمًا ما تَصبُّ في صالح تعزيز النقاش حول القضايا الرئيسة، تم السماح بنشر هذا التقرير على المستوى العام، كما أن حقوق التوزيع غير مقيدة.

يخضع هذا المنشور للمادة 17 من قانون الولايات المتحدة، البنود 101 و105، كما أنه ينتمي للمجال العام، ولا يجوز تقييده بحقوق النشر. يُرجى إرسال أي ملاحظات متعلِّقة بهذا التقرير، إلى العنوان التالي:

مدير معهد منشورات الدراسات الاستراتيجية

وكلية حرب الجيش الأمريكي، كلية حرب الجيش الأمريكي،

47 آشبورغ، كارلايل، PA 17013-5010.

يمكن تحميل كافة المنشورات الخاصة بمعهد الدراسات الاستراتيجية (SSI) وكلية حرب الجيش الأمريكي (USAWC) مجانًا من موقع معهد الدراسات الاستراتيجية، كما يمكن الحصول على نسخ مطبوعة

من هذا التقرير مجانًا، في حين يتم طلب المزيد من المواد من خلال تقديم طلب على موقع معهد الدراسات الاستراتيجية.

وقد يتم نقل منشورات معهد الدراسات الاستراتيجية أو طبعها جزئيًّا أو كُليًّا بالإذن والصلاحية اللذين تم منحهما لمعهد الدراسات الاستراتيجية وكلية الحرب التابعة للجيش الأمريكي، كارلايل، ولاية بنسيلفانيا. للتواصل مع معهد الدراسات الاستراتيجية؛ يُرجى زيارة موقعنا على الإنترنت على العنوان التالي: www.StrategicStudiesInstitute.army.mil

يقوم معهد الدراسات الاستراتيجية وكلية الحرب التابعة للجيش الأمريكي بإرسال نشرة شهرية عبر البريد الإلكتروني؛ وذلك لتحديث المعلومات لدى الجهات المعنية بالأمن القوميّ فيما يتعلَّق بالأبحاث الخاصة بالمحللين، والمنشورات الحديثة واللاحقة، والمؤتمرات القادمة تحت رعاية المعهد، كما توفِّر أيضًا كل نشرة إخبارية التعليق الاستراتيجي الصادر من قِبل أحد الباحثين المحللين، إذا كنت مهتمًّا باستلام هذه النشرة، يُرجى الاشتراك في موقع معهد الدراسات الاستراتيجية على:

www.StrategicStudiesInstitute.army.mil/newsletter

وضعت جميع المصادر والمواد المستخدمة في هذه الدراسة مِن الوثائق غير المصنفة لدى الحكومة، وتقارير وسائل الإعلام، والمؤلفات متاحة المصدر. يودُّ الكاتب أن يشكر عددًا من الأفراد والمنظمات التي تقدِّم المساعدات الهامة والملاحظات المفيدة خلال هذا البحث، وقبل كل شيء يتقدم بالشكر إلى أعضاء هيئة التدريس والطلاب والموظفين من برنامج الدراسات الأمنية في معهد ماساتشوستس للتكنولوجيا (MIT) ومختبر معهد ماساتشوستس لينكولن؛ وذلك لدعمهم وكرمهم خلال الزمالة التي عمل عليها المؤلف.

استضافت عدد من المنظمات المؤلِّف لإجراء المناقشات العامة حول مسائل الهوية، والتكنولوجيا، والقضايا الأوسع نطاقًا، التي تتعلق باستراتيجية الأمن القومي، وتشمل هذه المنظمات: وكالةَ الطب الشرعيِّ الدفاعيِّ والقياساتِ الحيويَّةَ، مركزَ علومِ الطبِّ الشرعيِّ الدفاعيِّ، وقيادةَ العملياتِ الخاصَّة الأمريكية، ونائب رئيس أركان الجيش لشؤون الاستخبارات، ووكالة المخابرات البرية القومية، والمركز الوطني للإعلام، ومشروع هوية الاستخبارات التابعة لمكتب وكالة الاستخبارات الدفاعية، وعدة مكاتب أخرى داخل مديرية الاستخبارات الوطنية. كما استفاد المؤلف كثيرًا من عشرات المناقشات المهنية والندوات التي قُدِّمت خلال القمة العالمية للهوية 2014.

على وجه الخصوص، يعترف المؤلف بالدعم الكبير المقدَّم من طرف السيد/ إدواك في مختبر معهد ماساتشوستس لينكولن، والسيد/ جيم شوفيلت من كلية الحرب التابعة للجيش الأمريكي، والدكتور/ باري بوسن وبرنامج الدكتور/ أوين كوت للدراسات الأمنية بمعهد ماساتشوستس للتكنولوجيا، وقد كان دعمهم ونقدهم للأفكار المقدمة في هذه الدراسة لا يُقدَّر بثمن، وأيُّ أخطاء في الحقائق أو التحليل ترجع للمؤلِّف وحده.

رقم الإصدار الدوليِّ ISBN 1-58487-703-0

تمهيد

خلال الخطاب الذي صدر مؤخرًا، الموجَّه لجامعة الدفاع الوطني عن مكافحة الإرهاب في الولايات المتحدة الأمريكية، حذر الرئيس الأميركي باراك أوباما أن :"*علينا تحديد طبيعة ونطاق هذا الصراع، وإلا فإنه هو الذي سيعمل على تحديدنا*"، أشارت تعليقاته إلى التحولات الهائلة في الجيش الأمريكي وجهاز الأمن الوطني منذ 11 سبتمبر 2001 (9/11)، وكان أبرزها التركيز التنفيذي الجديد على التهديدات التي يمثِّلها الفاعلون الدوليون "**من غير الدول**" (يقصد المنظمات) والمقاتلون الفرديون.

ويمثل هذا الإتجاه تحوُّلًا كبيرًا من منهجية عصر الحرب الباردة، التي تركِّز في المقام الأول على التهديدات التقليدية من الخصوم الرسميين "**الدُّول**"، واستراتيجية ترتيب الأولويات هذه نتج عنها مذاهب عسكرية جديدة تُركِّز على مهمة هزيمة الشبكات بدلًا مِن النماذج والابتكارات التقنية المصممة لتحديد ومراقبة واستهداف المقاتلين الفرديين في ساحة المعركة. هذا الإتجاه العملي جعل من مسألة الهوية مسألة هامة ومركزية لاستراتيجية الأمن القومي الأميركي، سواء بالكشف عن تهديدات فردية على الحدود، أو فصلهم في ساحة المعركة أو استهدافهم عبر المسافات بينهما.

في هذه الدراسة، يدرس العقيد/ **غلين فويلز** هذه السمة المميزة للصراعات الحديثة، وتحديدًا الابتكارات العقائدية والتقنية، التي أدَّت إلى ظهور هذا النموذج التنفيذي الجديد، وهو يصِف الدعائمُ الرئيسة للحرب الفردية، بما في ذلك زيادة الاستهداف على أساس الهوية؛ والدور الرئيس لتكنولوجيا المعلومات في قيادة هذه العمليات.

ويُسهِم هذا العمل في الحوار الهامِّ الذي يتعلق بالدروس المستفادة من السنوات العشر الأخيرة الخاصة بعمليات مكافحة الإرهاب العالمية إلى جانب اثنين من الحملات الموسَّعة لمكافحة التمرد (العراق، أفغانستان).

إنه يوفِّر دراسة حالة تفيد في الابتكار العسكريِّ في زمن الحروب، وذلك من خلال النظر في السياسات والاستراتيجيات التي تطوَّرت ردًّا على الخَصْم الجديد غير المتوقَّع. ويَختِم هذه الدراسةَ بمناقشة مُتعمَّقة تغطِّي مجموعةً واسعةً من التكنولوجيات الناشئة التي تقوم بتحديد الكيفية التي سيتم من خلالها الخوض في هذا النوع من الحروب في المستقبل.

دوجلاس سي. لوفليس، الابن

المدير

منشورات معهد الدراسات الاستراتيجية وكلية حرب الجيش الأمريكي

نبذة عن الكاتب

غلين جي، فويلز: هو ضابط مخابرات بالجيش وزميل كلية الحرب بالجيش الأمريكي في معهد ماساتشوستس للتكنولوجيا (MIT) وبرنامج دراسات الأمن ومختبر لينكولن MIT. وهو حاليًّا يخدُم في إدارة المخابرات في هيئة الأركان العسكرية الدولية، بمقرِّ منظمة حلف شمال الأطلسي في بروكسل، بلجيكا. خلال حياته المهنية، خدم في عدة مناصب في وكالة الاستخبارات الدفاعية، وفي هيئة الأركان المشتركة في البنتاغون، كمسؤول هامٍّ في غرفة العمليات بالبيت الأبيض.

وتضمَّنت مهامه العسكرية مهام متعددة في آسيا وأفريقيا والشرق الأوسط وأوروبا. وخدم سابقًا في منصب أستاذ مساعد في التاريخ في ويست بوينت. وفي وقت مبكِّر من حياته كان عضوًا في برنامج الصفِّ الرياضيِّ العالميِّ التابع للجيش، وقد كان تأهَّل مرَّتين في التصفيات الأولمبية الأمريكية للسباحة في عام 1988 والخماسيّ الحديث في عام 1996.

كما أنَّ العقيد/ فويلز هو مؤلِّف العديد من الكتب والمقالات الصحفية بشأن مجموعة من الموضوعات بما في ذلك التاريخ الدبلوماسي والتعاقد الحكومي، سياسة الاستخبارات والاستراتيجية العسكرية. العقيد/ فويلز هو خريج وست بوينت، حيث تم تكليفه ضابطَ مُشاةٍ في عام 1992. ويحمل درجة علمية متقدمة من جامعة فرجينيا وجامعة المخابرات الوطنية في واشنطن العاصمة.

ملخص

خلال عقد كامل من عمليات مكافحة الإرهاب العالمية واثنين من حملات مكافحة التمرد الممتد واجهت الولايات المتحدة نوع جديد من الخصوم؛ بدون زي رسمي، أو أعلام، أو تشكيلات، حيث أصبح تحديد واستهداف هؤلاء المقاتلين تحديًا عمليًا غير مسبوق، وأصبحت الأساليب المتبعة في حقبة الحرب الباردة غير ملائمة إلى حد كبير.

وأضحت هذه المشكلة هي المحفز لمدة عشر سنوات من التغيير المنهجيّ والتقنيّ والتنظيميّ الذي يقوم على الفكرة الرئيسة؛ بأن العناصر الفاعلة غير الحكومية والمقاتلين الفرديين كانوا مصدر قلق هائل لدى الأمن القوميّ، وبالتالي تعتبر أهدافًا عسكرية مشروعة. تم إعادة تحديد الأولويات الاستراتيجية لتتجه إلى نموذج منهجيّ جديد للحروب التي تركز على المهام التنفيذية وعمليات التحديد والفحص واستهداف المقاتلين الفرديين والعمل على هزيمة شبكاتهم.

وقد اتسم هذا النمط من الحروب بالأساليب التحليلية، التي تركز على التصنيف المنهجيّ للتهديدات وفصلها إلى مجموعات جزئية صغيرة، وصولًا إلى أدنى مستوى ممكن من الفصل الذي قد يصل إلى اعتبارهم مقاتلين فرديين في ساحة المعركة. وعندما لم يَعُد مِن الممكن التمييز بين الخصوم غير النظاميين من خلال الزيِّ الرسميِّ أو تشكيلاتهم العسكرية المعتادة، أصبحت "**سمات الهوية**" تقنية جديدة تستخدم في المعارك. وأصبحت البيانات البيو مترية، والأدلة الجنائية ومعلومات السيرة الذاتية عنصرًا حاسمًا في عملية الاستهداف العسكريِّ.

كما أن جمْع وتحليل هذه البيانات يتطلَّب تقنيات جديدة لإدارة المعلومات المصمَّمة للحدِّ من غموض الهُوية في ساحة المعركة، والمساعدة على اختراق الشبكات المعقَّدة، وتمييز العدوِّ من غيره. وتتطلَّب هذه الأنظمة أيضًا القدرة على معالجة البيانات وإرسال المعلومات المتعلقة بالهُوية عبر جهاز الأمن الوطنيِّ بأكمله.

تبحث هذه الدراسة في الابتكارات المنهجية والتقنية والإدارية التي تمَّ تطويرها بهدف الاستجابة لهذه التحديات التنفيذية الجديدة؛ حيث تدرس التحوُّل من التركيز على حُقبة الحرب الباردة التي تعتمد على الأساليب التقليدية؛ إلى مكافحة الشبكات والاستهداف على أساس الهوية، ويتم تحليل قرارات السياسات والخيارات الاستراتيجية التي كانت حافزًا على هذا التغيير؛ وتُختتم هذه الدراسة المتعمقة من خلال التكنولوجيات الناشئة التي من المحتمل أن تُشكِّل الكيفيةَ التي سيتم من خلالها الخوضَ في هذا النمط من الحروب في المستقبل.

صعود الحرب الإلكترونية: الهوية والمعلومات، والحروب الحديثة ذات الطابع الفرديّ

كلما أردت مهاجمة جيش، محاصرة مدينة، أو قتل شخص ما، يجب عليك أولا معرفة هويات كبار ضباط جهاز الدفاع، أعوانهم، زائريهم، حراسهم، والقائمين على سلامتهم...

سون تزو، فن الحرب

المقدمة

في أواخر ٢٠١٤، بلغت الولايات المتحدة رقم قياسي من خلال ضرب ٥٠٠ هدف خارج أرض المعركة، ضربات أَنْهت حياةَ ٣٦٠٠ شخص تقريبًا، في العقد الأخير. وفيما وراء هذه الأرقام، يمثل هذا الحدث مِثالًا على نَمطٍ جديد من حروب الدولة التي تقوم على القوة العسكرية التي تُطبَّق مباشرة ضد المقاتلين الفرديين بدلًا من التشكيلات، وهو ما يُسمَّى بـ «**القتل المستهدف**»، ولعل هذا الحدث هو المثال الأكثر وضوحًا للطابع الفرديِّ الذي تحوَّلت إليه أساليبُ الحرب الأميركية.

يقوم القائد الأعلى حاليًّا بشكل روتينيٍّ باستعراض واعتماد توجيه الضربات ضد مقاتلين فرديين محددين بأسمائهم، وهي ظاهرة لم يَسبِق لها مثيل في تاريخ الرئاسة، ومع ذلك، فإن هذا الإتجاه لا يقتصر فقط على جهود مكافحة الإرهاب على مستوى عالٍ، ولكن يُعبِّر عن التكامل الاستراتيجي الجديد الذي ارتقى بحالة المقاتل الفرديِّ، ليكون الشُّغل الشاغل للسياسة الأمنية الوطنية، وجعل استهداف هذه الكيانات هي المحرك الرئيس للابتكار المنهجيّ والتقني في ميدان المعركة.

وضعت هجمات 11 سبتمبر 2001 (9/11) واثنين من حملات مكافحة التمرد الولاياتِ المتَّحدةَ في مواجهة مع الخصوم، في وقتٍ لم تكن فيه الولايات المتحدة مستعدَّة لذلك بالشكل الكافي، لم يُحارب هؤلاء المعارضون الجدد باعتبارهم تشكيلات تقليدية أو من خلال معركة واضحة المعالم، بدلًا من ذلك، تم تنظيمهم كشبكات توزيع وخلايا صغيرة، تتألف من أفراد لا يمكن تمييزهم غالبًا عن السكان المحيطين،

وبدون زي رسمي وأعلام، وقد مثلت مهمة تحديد واستهداف هذه الكيانات تحديًا تنفيذيًّا غير مسبوق، وقد كان هذا النهج القتالي التقليدي غير ملائم إلى حدٍّ كبير، وردًّا على ذلك، بدأت أجهزة الأمن القومي للولايات المتحدة في إعداد ابتكارات تقنية وتنظيمية قائمة على الفكرة الرئيسة؛ بأن المقاتلين الفرديين يمثِّلون مصدرَ قلق للأمن القوميّ وهدفًا عسكريًّا مشروعًا.

ومع هذا النموذج التطبيقي الجديد، يصبح: **تحديد الهوية، الفحص،** واستهداف «**الأفراد المهمين**» والشبكات المرتبطة بهم، محورَ نمط جديد من الحروب .. الحرب الإلكترونية. (iWar)



ركائز الحرب الإلكترونية

إن (صعود الحرب الإلكترونية) هي عبارة عن دراسة حالة تتعلق بالابتكار العسكريّ، الذي يُركز على المهمة التنفيذية وعمليات التحديد والفحص، واستهداف المقاتلين الفرديين وشبكاتهم، وتتميز الحرب الإلكترونية بثلاثة عناصر متميزة: الطابع الفردي، والهوية، والمعلومات، توفِّر هذه الركائز إطارًا مفاهيميًّا لتحليل التغيرات الهائلة في المنهجية، والتكنولوجيا المستخدمة، والتركيز الاستراتيجي لتعريف كيف تحارب الولايات المتحدة في الخارج وتحمي حدودها من الداخل.

- **الطابع الفردي**

على مدى العقد الماضي، تحول جهاز الأمن القومي للولايات المتحدة من التركيز التقليدي على الخصوم العسكرية التقليدية إلى التركيز على التهديدات غير الحكومية والمقاتلين غير النظاميين، والشبكات القتالية المرنة سريعة التغير، وأدَّى هذا التغيير في الاستراتيجية لتبني أساليب تحليلية جديدة ومنهج تطبيقي يقوم على أساس التقسيم المنهجي للتهديدات، وصولًا إلى أدنى مستوى ممكن لدى المقاتل الفرديّ، في هذا النمط من الحرب، أصبح استهداف "الأفراد ذوي الأهمية العالية" يُمثِّل تهديدًا هائلًا للأمن القوميّ، والمحرك الرئيس للابتكار المنهجيّ والتقني في ميدان المعركة.

- **الهوية**

حيث إن الشبكات والمقاتلين الفرديين قد انتقلوا إلى المجال القتاليّ المحوريّ وأصبحوا يُمثِّلون تهديدًا على المستويات الأمنية الوطنية، وأصبح هناك ضرورة ملحَّة للتحديد والتمييز بين هذه الكِيانات، في عصر الحرب الإلكترونية، فلم يَعُد بالإمكان تمييزُ المقاتلين المعادين على أساس الحالة أو الزيِّ الرسمي، وحيث إن عملية الاستهداف العسكرية أصبحت ذات طابَع خاصٍّ، أصبح من الضروريّ ابتكار أنواع جديدة

من المعلومات والأساليب، التي تشمل المعلومات: البيوغرافية، البيو مترية، وبيانات الأدلة الجنائية، واستخدام تحليل الشبكة لربط هذه الهويات بالأماكن، والأنشطة، وغيرها من الجهات الفاعلة، أصبحت سِمات الهوية هي الميزة الفنية الجديدة في المعركة، وخط الدفاع الأول في نهج "قائمة المراقَبين" المتعلقة بالأمن القومي.

- **المعلومات**

يعتمد خوض معركة الحرب الإلكترونية على ثورة إدارة المعلومات، التي تتمحور حول التقنيات التي صُمِّمت للتمييز بين الجهات الفردية الفاعلة في ساحة المعركة والقدرة على تمييز الصديق من العدو، وتُعدُّ هذه المهام مختلفة تمامًا عن التحديات التحليلية الخاصة بحروب الحِقبة الصناعية، حيث تتطلَّب أدواتٍ وأساليبَ جديدةً لجمع وتجهيز وإرسال المعلومات الخاصة بالهوية عبر جهاز الأمن الوطنيّ بأكمله. إن الحاجة إلى تحديد وفحص واستهداف هذه التهديدات في الداخل والخارج جعلت إدارة المعلومات وتحليل البيانات هي أهم الأسلحة في عصر الحرب الإلكترونية.

تُعدُّ هذه الركائز الخاصة بالحرب الإلكترونية؛ عن النموذج التطبيقي الجديد الذي ظهر ردًّا على العدوِّ غير المتوقع الذي يحارب من خلال الشبكات بدلًا من التشكيلات العسكرية المعتادة. حيث لم يكن بالإمكان التعرف على هؤلاء المقاتلين بسهولة على أرض المعركة، حيث استغلوا عنصر عدم وضوح هوياتهم كمَيزة قتالية إضافية.

كما أن أنشطتهم لا تقتصر على ساحات القتال واضحة المعالم أو الأهداف العسكرية المعتادة. هذه الخصائص مكَّنتهم من مقاومة الميزة الأميركية الكُبرى في مناورات الحروب التقليدية، أو القوة الجوية، والخدمات اللوجستية. وأصبحت هذه المعضلة حافزًا لإعادة التغيير في استراتيجيات الأمن القومي استنادًا إلى الحاجة لتحديد وفحص، واستهداف هؤلاء المقاتلين الفرديين وشبكاتهم.

في هذا النموذج الجديد، لا يمكن قياس التقدم التنفيذيّ بمدى تدمير البنية التحتية المادية للعدوّ أو السيطرة على المساحات الرئيسة. وقد أدَّت هذه المفارقة إلى توجُّه الولايات المتَّحدة نحو استراتيجية من التكتيكات العسكرية القائمة على أساس التقسيم المنهجيّ للتهديدات؛ وصولًا إلى أدنى مستوى ممكن من التمييز.

وقد تطوَّر هذا المنهج إلى الأساليب القتالية التي تشمل «اندماج العمليات والاستخبارات لغرض تحقيق أهداف ذات قيمة عالية إلى أسلوب علميٍّ رفيع المستوى». وخلال صعود الحرب الإلكترونية، تم تعريف النجاح العملي من خلال تحديد هذه التهديدات الفردية في جميع أنحاء العالم، وفصلهم في ساحات المعارك، وفحصهم عند الحدود واستهدافهم عبر المسافات بينهما.

لم تتطوَّر أدوات وأساليب الحرب الإلكترونية نتيجة للتصميم الشامل الكبير، وبدلًا من ذلك تمَّ تحديد مسارات الابتكار من خلال الطوارئ التنفيذية، والتكيف التكتيكي، والأولويات الاستراتيجية الجديدة التي ظهرت خلال الاستجابة لعدو غير متوقع. وأدَّى ذلك إلى حِقبة من الابتكارات والتقنية التي تركِّز على مهمة تحديد واستهداف تهديدات العناصر غير الحكومية والمقاتلين الفرديين، أثار كلُّ هذا ثورةً لم يُسبَق لها مثيل من إدارة المعلومات وتبادُل البيانات عبر جهاز الأمن الوطني بأكمله.

كما أنه ساعد أيضًا على تنفيذ الكثير من التحولات البيروقراطية الكبرى التي عملت تدريجيًّا على تآكل العديد من الأساليب التقليدية التي تفصل ما بين العمليات العسكرية المختلفة، وأنشطة المخابرات الأجنبية، والمهام الأمنية المحلية. وتعبر هذه التغييرات عن الحسابات الاستراتيجية الجديدة التي وضعت تهديدات العناصر غير الحكومية والمقاتلين الفرديين على قَدَم المساواة مع الدول المعادية كمحرك لسياسة الأمن القومي الأميركي والابتكار العسكري.

التركيز على البحوث

تتألَّف هذه الدراسة مِن جزأين، يتناول القسم الأول الحرب الإلكترونية؛ كدراسة حالة للابتكار العسكريّ، ويتتبَّع مسارَ التغيير المنهجيِّ والتكنولوجي والتنظيمي داخل جهاز الأمن القومي الأمريكي ردًّا على نوع جديد من الخصوم. ويُحلِّل آليات الأجواء الأمنية لما بعد 11/9، وتحديد القرارات السياسية المحددة والخيارات الاستراتيجية التي أصبحت محفِّزات للتغيير والابتكار، كما يبحث كيف تطوَّرت هذه التغييرات من التحديات التي تُواجه عمليات محدَّدة للغاية لتحديد وفحص، واستهداف المقاتلين الفرديين في ساحة المعركة وعلى الحدود.

وأخيرًا: فإنه يُوضِّح كيف تتحدَّى هذه التغيرات الكثير من الافتراضات الأساسية التي واجهت إدارة الحرب في العصر الحديث.

الجزء الثاني هو أكثر تركيزًا على الناحية الفنية والتحليلية؛ حيث يركِّز على موضوع الابتكار العسكري، من خلال دراسة النتائج التي قد تقود إليها التوجهات الفنية الحالية، إذا ما واصلتِ الولايات المتحدة الأمريكية في مواجهة تهديدات الأعداء «من غير الدول» وغيرهم من العناصر الفردية. تَخلُص هذه الدراسة إلى المناقشة القائمة على السيناريو الذي يدرُس عدَّة مجالات من التكنولوجيا الناشئة التي قد تحدِّد كيفية شنِّ الحرب الإلكترونية في الجيل القادم.

دوافع الحروب الإلكترونية

كشفت هجمات 11/9 إلى حدٍّ كبير زيفَ اثنين من الافتراضات الدائمة بشأن استراتيجية الأمن القومي الأمريكي في حِقبة ما بعد الحرب الباردة، كانت أوَّل وجهات النظر التقليدية تنصُّ على المزيج من التماسك الداخلي الاجتماعي والثقافي، والاستقرار بين الدول المجاورة، وعزل الأراضي الأميركية عن أسوأ المخاطر الناشئة من الدول الفاشلة والإرهاب العابر للحدود.

وكان الافتراض الثاني هو أن القوة العُظمى أثناء خوض الحروب التقليدية القائمة على المناورات العسكرية وقوة السلاح، يُمكنها ردعُ التهديدات الرئيسة للأمن القومي الأمريكي، ومع ذلك، فإن صعود تنظيم القاعدة، واثنين من حملات مكافحة التمرد، والتهديدات الأمنية الداخلية المستمرة التي تفرضها العناصر الفاعلة غير الحكومية تؤدِّي إلى تفنيد كلٍّ من هذه الافتراضات.

وفي أعقاب 11/9، واجهت أجهزة الاستخبارات، الجيش والجهات الأمنية نوعًا جديدًا من العدوِّ الذي لا ينتمى إلى دولة ذات سيادة، ولا يرتدي زي رسمي، أو يسعى إلى أهداف جغرافية سياسية محدَّدة بوضوح، وقد أوضحت هذه التقارير طبيعة هذه التهديدات في مختلف الكتابات خلال الفترة الانتقالية لما بعد الحرب الباردة وربما كانت أكثر تنبؤية في كتاب «*الشبكات وحروب الشبكات*» للكُتاب/ جون اركيلا وديفيد رونفيلدت الإلكترونية.

في هذا الكتاب، وصفت الدراسة العناصر الفاعلة غير الحكومية المنظَّمة على أنها كِيانات مختلطة لا مركزية، التي شاركت في النزاعات منخفضة الحدَّة من خلال الاستفادة من المذاهب والتكنولوجيات القائمة على تصميم الشبكات، تحت شعار «حروب الجيل الرابع»، حيث تنبأ ويليام ليند تي إكس. هاميس، وآخرون؛ بأن هذه الشبكات والعناصر الفردية من المحتمل أن يحلُّوا محل الدولة كمحرك لنظام

عالمي جديد، كما ظهرت فكرة تم تحديدها لاحقًا من خلال أطروحة توماس فريدمان في "الأفراد فائقي الصلاحيات".

كل مِن هؤلاء الكتَّاب قاموا بإلقاء الضوء على حقيقة أن محاربة هؤلاء الخصوم تتطلَّب أن تقوم الدول بإعادة التفكير في المنهجيات والتقنيات غير ملائمة للعمليات غير المباشرة في ساحة المعركة التي تُسيطر عليها الشبكات والحملات الإعلامية بدلًا من التشكيلات والمناورة التقليدية، ووصفوا البيئةَ الأمنية الناشئة التي تحدِّدها الصراعات بين الجهات الحكومية وغير الحكوميين، أو الدول التي تستخدم العناصر الفاعلة غير الحكومية كوكلاء لها. وقد كان الرابط المشترك بين هذه التنبؤات هو حقيقة أن هؤلاء الخصوم الجدد سوف يصبحون منظَّمين على نحو شبكات موزَّعة غير منتظمة بدلًا من شبكات هرمية التنظيم.

إن تلك الصراعات تكون شِبه محليَّة أو عابرة للحدود في نِطاقها، وقد تميل العمليات إلى دمج المستويات الاستراتيجية والتكتيكية للحرب. الأهمُّ من ذلك أنَّ هؤلاء الخُصوم يكون من الصعب تحديد طبيعتهم ومواجهة استهدافهم. وتتطلَّب هزيمتهم مناهج تحليلية جديدة، وهياكل تنظيمية وتقنيات واستراتيجيات قتالية. ومنذ ذلك الحين تمَّ التحقُّق من صحة العديد من تنبؤات الحرب التي أعقبت التجربة الأميركية في العراق وأفغانستان والحملة الجارية ضد الإرهاب العالمي، ومؤخرًا في ما يسمَّى بـ «الصراعات المختلطة» التي تتميَّز بالقتالية اللامركزية وعدم انتظام الميليشيات التي لا تُعَدُّ جيوشًا احترافية نظامية.

في كل هذه النواحي تناضِل الولايات المتحدة لاحتواء وهزيمة الخصوم وَفْقًا للمنطق التنظيمي الذي يختلف كثيرًا عن التهديدات الرسمية، التي تعتمد منهجيًّا على أساليب حِقبة الحرب الباردة، بدلًا من ذلك، كان هؤلاء الخصوم الجدد يَظهرون بشكل هيكليّ معقَّد ويفتقرون إلى صلاحيات المراكز التنفيذية الواضحة، هذه الكِيانات تَستخدم تكتيكات شديدة الغرابة واستراتيجيات التكيف التي يُعتبر من الصعب تحليلُها. بالإضافة إلى ذلك، فقد كانوا بارعين بشكل خاص في استغلال التكنولوجيات

التجارية، والاتصالات، والشبكات المالية لتوسيع نفوذهم. وفي بعض الحالات، كانوا يقتربون من «**القدرة التخريبية التي تتمتَّع بها الدول**» لتنفيذ هجمات ذات تأثير عالمي.

أظهرتْ متطلِّبات شَنِّ هذا النوع الجديد من الحروب تحديًا مُختلِفا تمامًا عن أساليب خصوم عصر الحرب الباردة. قبل 11/9، كانت أساليب المخابرات الأمريكية ما زالت تعكس في المقام الأول التراث المنهجيّ الخاص بنموذج «ترتيب المعركة» الذي يركِّز على الوحدات والمعدات والتشكيلات، والنماذج المنهجية الثابتة.

وتركَّزت أولويات المجموعة على التحليل الفني طويل الأمد على قدرات التهديد ورصد المؤشرات الاستراتيجية والتحذيرات، ومع ذلك، طالبت حملات الولايات المتحدة في العراق وأفغانستان بنهج جديد تمامًا مع مزيد من التركيز على «العوامل البشرية» والتحليل الشبكيِّ، وتتمحور المناهج البشرية في مكافحة التمرد حول المطالبة «ليس فقط بالقدرة على التعرف على هويات الأفراد، ولكن أيضًا فَهْم البِنية الاجتماعية من حيث العلاقات الاجتماعية بين السكان»؛

ونتيجة لذلك خَضعتْ أجهزةُ الاستخبارات وقوَّات الجيش إلى تحوّل كبير على أساس النظريات القتالية، التي وضعتِ الشبكاتِ في مركز التحدي التحليلي والتنفيذي، وهذا يعني أيضًا أنه للمرة الأولى في الحرب الأميركية الحديثة أصبحت مسألة الهوية نقطة جوهرية كمدخل للبيانات و«علامة» عملية، والتي أضحت حساسة وتحت المجهر، والعزل، واستهداف المقاتلين الفرديين في ساحة المعركة وإيقافهم على الحدود.

الحرب الإلكترونية باعتبارها استراتيجية أمن قومي

لم تنشأ الحرب الإلكترونية على هيئة تصميمٍ معين أو استراتيجية مُتعمّدة، بدلًا من ذلك، تطورت تدريجيًّا وبطريقة مُجزَّأة كنتيجة التكيف المخصص والخيارات السياسية المتزايدة في السنوات التي تلت أحداث 11 سبتمبر، ظهرت ركائز الحرب الإلكترونية في قلب الأساليب التي اتبعتها الدولة لاستهداف ومكافحة الإرهاب من خلال المنهجيات القتالية المعتمدة في العراق وأفغانستان، وكأساسٍ لاستراتيجية الأمن القوميِّ المبنية على أساس نُظُم فحص الهُويَّة.

قدَّم تفويضُ استخدام القوة العسكرية (AUMF) حافزًا أوليًّا مهمًّا للحرب الإلكترونية؛ وذلك عبر السماح باستخدام القوة ضد «الدول والمنظمات أو الأشخاص»، وبالتالي وضَع سابقةً قانونية لاستهداف المقاتلين الفرديين كعنصر من عناصر الاستراتيجية الموسّعة لمكافحة الإرهاب، هذا الخيار السياسيُّ يظهر في نهاية المطاف من خلال تحديد استراتيجية مُركزة لمكافحة الهجمات الإرهابية، فيما يُسمَّى بـ «القتل المستهدف»، وأبرزها يتمُّ من خلال هجمات الطائرات بدون طيَّار في باكستان واليمن والصومال، ضد أهداف القيادات العليا والشخصيات التنفيذية الرئيسة.

وقد تمَّ تطويرُ هذه المنهجية التي يتم استهدافها تدريجيًّا مع مرور الوقت، وخاصة التحول من أسلوب يعتمد على أساس الضربات العامة، تُجاه عمليات هجومية تقوم على أساس أكثر تركيزًا لاستهداف نمط محدَّد من «الشخصية» ضد أفراد محددين ومعروفين على نحو خاصٍّ.

على الصعيد الداخلي، أصبح نموُّ الحرب الإلكترونية أكثرَ وضوحًا من خلال ظاهرة »قائمة المراقبة« وبرامج الفحص على أساس الهُويَّة التي أصبحت سِمة أساسية في استراتيجية الأمن القومي بعد أحداث 11/9 خلال الفترة الماضية، وقد تم إضافة هُويات الملايين من الأفراد في قوائم المراقبة، مع زيادة

المعلومات المفصَّلة عن السيرة الذاتية لكل شخص، وعناصر الاستدلال البيولوجيّ (البيو مترية) والتاريخ الفعليّ، والشبكات الممتدَّة من الرابطات والاتصالات. وقد أصبحت هذه البيانات هي أساس المعلومات لبرنامج الفحص على أساس الهُوية، التي تهدُف إلى تسليط الضوء على التهديدات الفردية والتركيز على المخاطر المحتملة لشبكات النقل والبنية التحتية الأساسية، ومختلف عوامل الأمن الداخلي.

وبخلاف استهداف ومكافحة الإرهاب والدفاع الوطنيّ؛ أصبح نموذج الحرب الإلكترونية أكثر وضوحًا من خلال تطور المنهجية العسكرية والتقنيات والأساليب القتالية المستخدمة في العراق وأفغانستان، وقد أثَّر ذلك على الأساليب المركزية ومنهجيات الاستهداف التي تطوَّرت تدريجيًّا خلال هذه الحملات، من خلال نظرية الشبكات والأساليب التحليلية؛ للتأكيد على دور المجموعات الصغيرة، واللاعبين الفاعلين الرئيسين، والعناصر الفردية باعتبارها متغيرات حاسمة في دعم وتأسيس الأمن على المستوى المحليّ.

أدَّى هذا التركيز التطبيقيُّ إلى عَقدٍ كامل من الابتكار التكنولوجي العسكري المتسارع، الذي قدَّم مجموعةً من الأدوات الجديدة لميدان المعركة، وهي الأدوات التي صُمِّمت خصيصا لدعم عمليات معالجة الهوية والاستهداف على المستوى الخاص، بما في ذلك الطائرات بدون طيار، القياسات الحيوية، والطب الشرعي، ونُظم معالجة البيانات المتقدمة. هذا النموذج الجديد يمثِّل إعادة توجيه رئيسي للتركيز العسكري بعيدًا عن أساليب الحرب التقليدية، نحو نموذجٍ جديد لحروب الدولة التي تعتمد على التحديد والفحص، واستهداف المقاتلين الفرديين.

إن وراء التقنيات والنظريات الجديدة، يظهر نموُّ الحرب الإلكترونية التي تمثل خروجًا عميقًا عن الافتراضات الأساسية لنظام «**وستفاليا**» الذي حدَّد سياق حروب الدول لأكثر من 300 سنة منذ نهاية حرب الثلاثين عامًا، حددت هذه اللحظة التاريخية نقطة التحول الهامة من الصراعات الجماعات المأجورة الخاصة، نحو أسلوب الحرب الحديثة، التي ظهر فيها المقاتلين باعتبارهم كأدوات للدولة نيابةً عن القادة السياسيين، وهو ما يُشير إلى "انحسار الطابع الشخصي" للصراع، حيث يَتْبع الجنود هُويَّة جماعية باعتبارهم أعضاء في جيوش احترافية.

تُعتبر أطروحة «**جان جاك روسو**» الخاصة بالسلطة السياسية المفصلية، هي التي تُعبِّر بالشكل الأفضل عن أهمية هذه المرحلة الانتقالية، مشيرًا إلى أن الحروب الحديثة لم تَعُد:

> ***عَلاقة بين رجل واحد وآخر، ولكن هي علاقة بين دولة وأخرى، يكون فيها الأفراد أعداء فقط عن طريق الصدفة ليس كأشخاص، ولا كمواطنين، ولكن كجنود.***

قام هذا المفهوم بتقديم الأساس الفكري للتطور التالي للتصنيفات القانونية التي تُنظِّم معاملةَ السجناء والجنود الجرحى والمدنيين في ساحة المعركة، وأساس تحديد الإطار الشرعيِّ للمعارك، وفي إطار معاهدة وستفاليا، أصبح الجنود أعضاء بشكل عام في جيوشهم الوطنية من حيثُ الوضع القانوني وكذلك المظهر.

وقد ظهر الزيُّ الرسمي لتمييز الجنود عن غيرهم من المدنيين، وتوفير إطار عمليٍّ للاستهداف المشروع للعدو، والحماية أثناء فترة الحرب. في هذا النمط من الحرب؛ لم تَعُد الامتيازات القتالية والالتزامات وقواعد الاشتباك مرتبطة بالهُوية الفردية، وإنما ترتبط بالوضع العامِّ للجنود باعتبارهم أعضاء في نظام الدولة. ومع مرور الوقت تطوَّر هذا النمط إلى الإطار المعياريِّ الذي يحكم سير حروب الدول، واتفاقيات الاستهداف العسكري.

منذ أحداث الحادي عشر من سبتمبر، تم تحدَّى هذا التصور مباشرةً من خلال سلسلة من الصراعات خاضتها الولايات المتحدة الأمريكية ضد الشبكات بدلًا من الدول، وضد قواتٍ معاديةٍ تتألَّف من "محاربين معادين غير محترفين"، وفي هذا السياق، فإن الولايات المتحدة قامت بإجراء عمليات عسكرية مستمرة ضد مقاتلين يعتبرون غير مؤهلين قانونيًّا للامتيازات المفترضة للمقاتلين، نتيجةً لدعم الجماعات المسلحة غير النظامية في سير العمليات القتالية.

تسبَّب هذا الأمر في خلق غموضٍ تطبيقي بحيث أصبح الأسلوب التقليدي للاستهداف القائم على الحالة غير فعَّال على المستوى الفعليِّ، وقد قام الجيش الأمريكي بتطوير المنهجيات القائمة على الطابع الفرديِّ لتقييم عوامل التهديد، والاستهداف على أساس الهُوية حيث لم يَعُدِ الخصوم مقاتلين "بالمفهوم العام".

ويعكس هذا النموذج التطبيقيِّ الجديد إضفاء الطابَع الشخصي على الحروب؛ حيث أصبح استخدام القوة العسكرية الشرعية "مرتبطًا بالأحكام شِبه القضائية التي تصدُر بشأن أعمال وأدوار الأفراد في المجموعات المحددة للعدو"، ويستند الاستهداف بشكل متزايد على تقييم فردية المقاتلين المحددين، ويتم تحديد ذلك من خلال تحليل الأدلة ذات الأهمية التطبيقية داخل الأدوات العامة للشبكة.

ويعبِّر ذلك عن التحول الجِذريِّ في معايير الاستهداف المطبقة على أرض المعركة الحديثة. وقد ذلك أيضًا على تغيير كيفية جمع المعلومات وتحليلها، واستخدامها في دعم العمليات العسكرية، مثل ظهور أسلوب "الاستهداف القائم على الأدلة".

إن صعود الحرب الإلكترونية قد يتحدَّى أيضًا قاعدة ضِمنية أخرى لمعاهدة وستفاليا، على وجه الخصوص قد يتحدَّى الحظر العام ضد الاستهداف المباشر للقيادة السياسية كأسلوب من أساليب الحرب الحديثة. مع تزايُد الجيوش المحترفة، لم يَعُدِ القادة السياسيون يقودون الجيوش مباشرة في المعركة، وبالتالي فإن ذلك يخلق تمايزًا واضحًا بين أولئك الذين يقومون بإدارة الحرب على مستوى السياسات، في مقابل أولئك الذين يقومون بخوضها فعليًّا في أرض المعركة.

وهكذا فإن التطبيق الفعليَّ لذلك يعني بأن "ضربات القيادة" ضد الشخصيات السياسية أو الأهداف غير التنفيذية عمومًا لم تتطوَّر باعتبارها عنصرًا أساسيًّا ضمن الاستراتيجية العسكرية، ومع ذلك فقد تعقَّدت هذه الاتفاقية من خلال غموض التمييز بين القيادة التنفيذية و"السياسية" داخل الجماعات من غير الدول؛ على سبيل المثال:

قامت الولايات المتحدة بشنِّ هجمات قاتلة تستهدف الأفراد المعروفين بشكل عام باعتبارهم زعماء دينيين أو متحدثين باسم الجماعات المتطرفة، وذلك على أساس أنهم يقومون بتقديم الدعم الأساسيِّ للأنشطة الإرهابية، ومع ذلك، فإن التفسيرات التقليدية لقانون النزاعات المسلَّحة تحدِّد بشكل عام الاستهداف العسكريِّ ليكون محصورًا على المشاركين مباشرة في الأعمال العدائية، في حين يتم إعفاء الأفراد مثل رجال الدين أو غيرهم من المدنيين العاملين في أدوار ومهام غير تنفيذية.

وقد عمِلت منهجية الحرب الإلكترونية على تعقيد هذه الفروقات، حيث إنَّ المعايير القائمة على الحالة أو الوظيفة لم تَعُد تقدِّم نموذجًا واضحًا لاستهداف هؤلاء المقاتلين الفرديين.

هناك أيضًا الآثار الكبرى للسياسة، حيث يكون المقاتلون الفرديون في بؤرة تركيز الاستهداف الفعليِّ بدلًا من التشكيلات التقليدية. وقد خَلَق نموذج الحرب الإلكترونية نِطاقًا محددًا للصراع مع وجود القليل من الحدود الجغرافية السياسية، القضائية، أو المؤقتة الملحوظة، وهذه الحقيقة تم الاعتراف بها ضمنيًّا من قِبل الإدارات الأمريكية المتتالية.

كما لاحَظ أحد المراقبين في الآونة الأخيرة، قيام حرب ضد مجموعة متغيرة باستمرار من العناصر الفاعلة، الذين يتنقلون بحرية من مكان إلى آخر ومن مؤسسة إلى أخرى، بحيث لا يمكن تحديد أيِّ "عدو" واضح المعالم كما أن الصراع لا يمكن أن ينتهي بمعاهدة سلام، في مثل هذا الصراع لم يَعُد لدينا معنى واضح أو مستقرٌّ لمصطلحات **ساحة المعركة، المقاتلين، والأعمال العدائية**، وقد ظهرت هذه المعضلة بشكل حاد في الخلافات الدبلوماسية والقانونية الراهنة، التي تدور حول قضية الاحتجاز العسكري غير محدَّد الأجل.

بمقتضى معاهدة **وستفاليا**، يتم إنهاء الحرب في إطار مُعترَف به، والذى يتم فيه التفاوض بشأن شروط السلام، وعملية التطبيع لإخلاء ساحات القتال وعودة المقاتلين لأوطانهم، ومع ذلك، لم تلتزم الحملات في عصر الحرب الإلكترونية بهذه الاتفاقيات التقليدية، وقد أسفرت هذه الصراعات عن أفواج من المحاربين المسافرين، الحريصين على تطبيق مهاراتهم وخبراتهم عبر مسارح متعددة من عمليات الصراع وأعمال الإرهاب الموجهة خارج مناطق القتال المعترف به.

هذا الوضع قد غيَّر بشكل أساسيٍّ الأهمية الفعلية للهوية والاستراتيجيات اللازمة بشكل جِذري على أساس المراقبة المستمرة للمقاتلين المهنيين، داخل وخارج ساحة المعركة. وقد أظهرت مشكلة عودة المدانين إلى الجريمة والانتقال العالميِّ المستمر للمقاتلين؛ معضلة أمنية جديدة تمامًا تُواجه الدول القومية، وهي المعضلة التي لا تُقدِّم أي مسار واضح نحو النصر العسكريِّ التقليدي أو إجراءات تسريح المقاتلين.

ويعكس هذا الوضع ما أسماه بعض المراقبين بـ "تهجين الحرب" باعتبارها مجموعة من العمليات العسكرية التي تمتدُّ على نحو متزايد بين مختلف الأنشطة القائمة بين النقيضين وهما الحرب والسلام، وكنموذج لحروب الدول، فإن الحرب الإلكترونية تحتلُّ هذه المنطقة الرمادية بين الحرب التقليدية ونفاذ القانون، حيث تتميَّز بخصائص لدى كل منهما، ولكن دون القواعد الإجرائية والسياق القانوني الواضح، وبالنسبة للولايات المتحدة، فإن تلك الفكرة قد اكتسبت خصائصها عبر الإجراءات العسكرية التقليدية المستمرة، التي قد تكون متكاملة، مثل الإضرابات الحركية والاحتجاز في ساحات القتال، والتي تترافق مع نَهْج إنفاذ القانون على أساس تحليل الأدلة والاعتقال والملاحقة القضائية.

وقد تطوَّرت هذه الأساليب إلى حد كبير كحلٍّ افتراضي لخوض الحرب عبر ساحات قتال لا محدودة، حيث يمكن ملاقاة "المقاتلين سواء على أرض المعركة، أو في قائمة صعود الطائرة في المطارات"، وقد لاحَظ بعض العلماء أن هذا الوضع الجديد للصراع الذي تخوضه قوات الدُّول ضد المقاتلين الفرديين، لا يتمتَّع بالإطار القانوني القائم الذي يمكن على أساسه إصدار قرارات استهداف مشروعة، وفي الواقع، فإن الإتجاه التطبيقيَّ نحو الاستهداف الشخصيِّ على أساس الهُوية يتحدَّى العديدَ من الاتفاقيات التي حدَّدت استخدام القوة العسكرية من قِبل سلطات الدولة على مدى أجيال.

وباختصار، فإن صعود الحرب الإلكترونية يمثِّل أسلوبًا جديدًا لحروب الدول التي يَحُلُّ فيها تهديد المقاتلين والشبكات الفردية محلَّ التشكيلات التقليدية في قلب استراتيجية الأمن القومي، ويتناول القسم التالي الحرب الإلكترونية كمثال للابتكار المنهجي، ويبحث في كيفية تطور المنهجيات القتالية منذ أحداث الحادي عشر من سبتمبر كاستجابة لهذا النوع الجديد من الخصوم.



أصبحت أُسس نموذج الحرب الإلكترونية واضحة للعَيان خلال العقد الأخير من الابتكار المنهجيِّ، لا سيما فيما يتعلَّق بنهج الولايات المتحدة لاستراتيجيات مكافحة الإرهاب ومكافحة التمرد، وبينما تمثِّل هذه المهام مجموعة متمايزة من الأهداف والأساليب، فإنها تشترك على المستوى المفاهيمي في قاسم مشترك مهم، يتمثَّل في وضع الشبكات والعناصر الفاعلة الفردية في مركز التحدي التحليلي والتطبيقيِّ، إن فحص هذا التطور المنهجيِّ يعتبر اختبارًا مفيدًا لفَهْم كيفية تَطوُّر هذه المفاهيم على مرِّ الزمن لتُكوِّن الفكرَ المؤسسي للجيش، وتوضِّح لنا هذه التحولات التطورية منظورًا مهمًّا في كيفية فَهم القادة التنظيميين لطبيعة خصوم مرحلة ما بعد 11/9 والأساليب اللازمة لإلحاق الهزيمة بهم.

من بين الدروس الأولى المستفادة من الحملات في كُلٍّ من العراق وأفغانستان هو أن "نهج الحرب التقليدية غالبًا ما يكون غير فعَّال عندما يطبَّق على العمليات بخلاف الحالات القتالية الرئيسة، مما اضطر القادة إلى إعادة تنظيم الطرق والوسائل لتحقيق النتائج المرجوة"، ويوضِّح دليلُ الاستهداف الأخير الخاصُّ بالجيش أن التركيز التطبيقيَّ للحرب التقليدية يدور حول "إيجاد وتدمير السفن، تشكيلات الدبابات، أو البنية التحتية".

وفي المقابل، يوضِّح الدليلُ أنه خلال مكافحة التمرد، فإن المهمَّة الأكثر صعوبة هي ببساطة تحديد ماهية العدو، وتعكس هذه التحديات التطبيقية الجديدة، الملاحظات المذكورة في تقرير صادر عام 2007 من قبل مجلس العلوم الدفاعية الذي أقرَّ بأن مهمة تمييز هُويات المقاتلين قد أصبحت مصدر قَلَقٍ مُتزايد الأهمية في ساحة المعركة، وخصوصًا باعتبارها أساليب قائمة على أساس الحالة "تقلّص مُعدَّل استخدامها والاستفادة منها".

وقد أدَّت هذه التحديات إلى قيام الجيش الأمريكي بإجراء تغييرات منهجية رئيسة استمرَّت عقدًا كاملًا من الزمن، وهي التغيرات التي تركِّز على إيجاد وسائل أفضل لشنِّ حرب ضد الشبكات بدلًا من التشكيلات، واستهداف المقاتلين الفرديين بدلًا من المجموعات الكاملة، وحتى مع قيام قوات الولايات المتحدة باتباع نظرية مكافحة التمرد، مع التركيز على معايير الحوكمة والاستقرار، والتركيز التطبيقيِّ يومًا بعد يوم في كلٍّ من العراق وأفغانستان على التوجه نحو الجهود التي تستهدف "تحديد وفَصْل العناصر التي لا يمكن التصالح معها عن العناصر القابلة للتصالح"، يرتكز أحدُ العناصر الرئيسة لإرساء الأمن المحليِّ في هذه الحملات على الجهود الحثيثة لتحديد وفصل العناصر الفاعلة الرئيسة ضِمن شبكات المتمردين، وتحييد شبكاتهم، وإجراء عمليات القتل/ الاعتقال ضد الأهداف من المستوى الأولى.

تطوَّرت منهجية الاستهداف المسمَّاة "البحث، الإصلاح، الإنهاء، الاستخدام، التحليل، والتفكيك" (F3EAD) كمنهجية مفضَّلة لتحديد وتوظيف هؤلاء الأفراد ذوي القيمة العالية (HVI). وقد طبقت قوات الولايات المتحدة في كل من العراق وأفغانستان منهجية F3EAD مع نجاح كبير ضد شبكات المتمردين والخلايا الإرهابية، وفي العراق، تم استخدام هذه الأساليب للاستهداف القائم على الشبكات لتطوير جميع المصادر الاستخباراتية وتوفير "الوعي بظروف البيئة المحلية، والشبكات الاجتماعية، وصناع القرار الرئيسين، ودوافعهم"، وربما كان هذا النهج هو الأكثر تطبيقًا خلال محاولة تَتبُّع، واستهداف وقَتل الزعيم الإرهابيِّ أبو مصعب الزرقاويِّ، ومن أجل دَعْم العمليات المستقبلية، يَصِف الجنرال "ستانلي ماكريستال" عملية التنفيذ المتكاملة والمحكمة بأنها تقوم على أساس ما يلي:

المُحلِّلين الذين وجدوا العدو، الطائرات بدون طيار التي حدَّدتِ الهدفَ؛ الفِرق القتالية التي أنهتِ الهدفَ عن طريق اعتقاله أو قتله؛ المتخصصين الذين استغلّوا المعلومات الاستخباراتية الناتجة عن العملية الهجومية، مثل

الهواتف المحمولة، والخرائط، والمعتقلين؛ ومحللي الاستخبارات الذين حولوا هذه المعلومات الأولية إلى معرفة قابلة للاستخدام.

في أفغانستان، وفيما بين عامي 2009 و2011، تم تطبيق نَهْج مماثل في استهداف شبكات المسلحين، وذلك باستخدام الأساليب التي مكَّنت من زيادة قَدْرها خمسة أضعاف في الغارات المركزة والمصممة لاعتقال أو قَتْل فرد أو مُتمرِّد على مستوى عالٍ، وبخلاف المقاتلين النَّشطين، قد تم تطبيق هذه الأساليب أيضًا للاستهداف غير الحركي ضد مُروِّجي المخدرات والشبكات الإجرامية كوسيلة للحدِّ من الدعم المالي لشَبكات المتمرِّدين، ومنذ ذلك الحين تم إدماج منهجية F3EAD في مبادئ الاستهداف التقليدي للجيش، والتي أصبحت جزءًا من برامج التدريب المؤسسية للجيش.

وفي حين تم تطوير منهجية F3EAD على وجه التحديد باعتبارها نهجًا عمليًّا للاستهداف على أساس الشخصية، فقد تطوَّرت ضِمن إطارٍ مفاهيميٍّ أكبر استنادًا إلى نظرية "هاجم الشبكة" (ATN)؛ حيث تُعتبر نظرية "هاجم الشبكة" (ATN) مثالًا واضحًا على التطور المنهجيِّ الذي يركِّز على التقسيم الجزئيِّ لساحة المعركة والتحليل القائم على الشبكة لدعم الاستهداف.

حيث ظهرت نظرية (ATN) أصلًا باعتبارها نهجًا تحليليًّا لمكافحة شبكات العُبُوَّات الناسفة (IED) وصُمِّمت من أجل العمليات الهجومية المركَّزة ضد الشبكات المعقَّدة التي تتألَّف من الممولين، وصناع العُبُوَّات بدائية الصنع، والمدربين، والبِنية التحتية الداعمة، كما أكَّدت نظرية (ATN) استخدام المصادر الاستخباراتية المتخصِّصة والطرق التحليلية لتحديد العُقد الرئيسة والروابط التنظيمية في شبكات العدوّ. وكجزء من هذه العملية، فقد قدَّمت نظرية (ATN) إطارًا يعمل على إعداد تصنيفات فرعية للجهات الفاعلة الفردية ضِمن مخطَّط تحديد مستويات الأولويات المستهدَفة.

على سبيل المثال، تتضمَّن أهدافُ المستوى الأول القياداتِ العليا، وتتضمَّن أهداف المستوى الثاني العناصرَ الوسيطة ذات الاتصالات بالوسطاء وعامة الناس، وتتضمَّن أهداف المستوى الثالث بشكل رئيسٍ الجنودَ ذوي المهارات المتدنية وأصحاب التهديدات العامة ضِمن السكان، وقد تم تطبيق أشكال مختلفة من هذا النهج الأساسي خلال مجموعة متنوِّعة من المهام، مِثل تتبُّع (جوزيف كوني) وعناصر (جيش الرب للمقاومة) في أوغندا، وتحليل انتشار نفوذ (بوكو حرام) في نيجيريا، وفَهْم أنماط تمويل الإرهاب من قِبل تُجَّار المخدرات في أمريكا اللاتينية، إن تطوير أساليب منهجية F3EAD ونظرية ATN يعكِس التطورَ النظريَّ والتكاملَ الأكبرَ لتحليل الشبكات الاجتماعية (SNA) في الإتجاه التطوري العسكري.

إنَّ استخدام نظام تحليل الشبكات الاجتماعية لتفكيك بِنية الشبكات المعقَّدة قد سبق الاستخدام المؤخر لذلك من قِبل الجيش الأمريكي، وذلك بواسطة أبحاث علمية يعود تاريخها إلى عام 1960، ومن أبرز أعمال هؤلاء الرواد المبكرين كان بحث (ستانلي ميلغرام) لظاهرة "العالم الصغير" ونظريات "تفكيك الوساطة الهيكلية" التي تَصِف ديناميكية الشبكات الاجتماعية المعقدة، وفي الآونة الأخيرة، فإن الباحثين مثل (دنكان واتس) قاموا بتوسيع تطبيق نظرية الشبكة من خلال إظهار أهميتها بالنسبة لظواهر مثل عدوى المرض، وسلوك المستهلك، وديناميات التأثير الاجتماعي.

وخلال عام 1990 اتَّسَع استخدامُ أساليب SNA على نِطاق أوسعَ لإنفاذ القانون وتحليل أنماط الجريمة؛ ومع ذلك، فإنها ظلَّت إلى حدٍّ ما على هامش أساليب التفكير المنهجيِّ العسكريِّ، وكان الأدميرال (آرثر كيبروسكي) من الأوائل بين القادة العسكريين في تطبيق هذه المفاهيم مباشرة خلال الاستراتيجية القتالية في عمله الهام "*الحروب المتمركزة حول الشبكات*"، واقترح مفهومًا للحرب متمركزًا حول الشبكات باستخدام معايير استشعار موزَّعة والاستهداف الدقيق، ومع ذلك، فإنه في ذلك الوقت لم يُتصوَّر تلك الطرق التي تستخدم خصيصا في سياق مكافحة التمرد أو استهداف المقاتلين الفرديين.

أصبحت هجمات 11/9 محفزًا أساسيًّا لاستخدام أساليب نظام تحليل الشبكات الاجتماعية SNA بشكل كامل في السياق المهني السائد الخاص بالاستراتيجية العسكرية وعمليات الاستهداف، وكانت أولى الأعمال في هذا المجال كتاب (مارك سيغمان) بعنوان "فهم شبكات الإرهاب"؛ فقد قام بتطبيق نظام تحليل الشبكات الاجتماعية SNA كإطار صريح لفَهْم أنواع جديدة من الخصوم، وفي عام 2006 تم نشر دليل الجيش لمكافحة التمرد الذي يعكس هذه التأثيرات، ويجلُب أساليب SNA بالكامل في الإتجاه المنهجيّ، وقد لا حظ (جون ناجل) أحد مهندسي هذا الإتجاه أن إدراج أساليب SNA لَعِب دورًا حاسمًا في القيادة:

"يُعدُّ جهاز المخابرات التابع للجيش بعيدًا عن التركيز على تحليل وحدات العدو التقليدية، ومُتَّجهًا نحو الفَهم القائم على الشخصية لشبكات الأفراد ذوي السلطات الفائقة"

وقد قام دليل مكافحة التمرد الجديد بوصف نظام تحليل الشبكات الاجتماعية SNA بأنه "أداة فعَّالة لتقييم التهديد"، وعرض مُفردات جديدة في المصطلحات التطبيقية العسكرية، مِثل مصطلحات: البِنية المركزية المحيطية، والكثافة المركزية، والتماسك، والتجميع، وتصوُّر الشبكة، وقد طُبِّقت هذه الأفكار مباشرة في مهمَّات تحليل الشبكات الإرهابية والمتمردة، وتحديد الفاعلين والمؤثرين الرئيسيين في ساحة المعركة، وكانت الفكرة البارزة لتطبيق نظام تحليل الشبكات الاجتماعية في عملية الاستهداف هي كيف أنَّ "القبض على أحد المسلحين" الذي يتمتَّع باتصالات عالية المستوى داخل شبكة متمردة كثيفة؛ يُمكن أن يساعد عملية مواجهة المتمردين على تحييد الهيكل التنظيمي الأكبر بشكل نظاميٍّ.

وفي سياق عمليات مكافحة التمرد ومكافحة الإرهاب، يُقدِّم نظامُ تحليل الشبكات الاجتماعية SNA الإطارَ المفاهيميَّ لتحليل شبكات العدوِّ، وتحديدَ الأدوار الوظيفية والمواقف التنظيمية، والجهات الفاعلة المؤثرة، وعلى المستوى التكتيكي، قد دعَمتْ نظرية تحليل الشبكات الاجتماعية SNA الحاجةَ العملية

لتطبيق تحليل "نمط الحياة" وتطوير الروابط المتَّصلة ومصفوفات الأنشطة، وقد مكَّن هذا أيضًا من التصور التفصيليِّ للشبكة عن طريق تحديد الشخصيات الرئيسة، والعادات، والمواقع، وحركة الطرق، والمعاملات المالية وصولًا إلى مستوى المقاتل الفرديِّ، هذه المعلومات شكَّلت أساسَ "مجلدات معلومات الهدف"، وهو الأسلوب المفضَّل لتمثيل العُقد الفردية بشكل نظاميٍّ داخل شبكات الخَصم.

تمَّ تطويرُ نتائج المخابرات من خلال أسلوب استهداف HVI القائم على تحليل الشبكات الاجتماعية عبر المعلومات القابلة للتطبيق، بما في ذلك الوصف التفصيليِّ الماديِّ للأهداف الفردية وتاريخ السيرة الذاتية، والعلاقات العائلية، والبيانات البيومترية، وأرقام الهاتف الجوال، وحتى أوصاف السيارة، وتُعَدُّ هذه الأساليب بشكل كبير كعنصر أساسيٍّ للنجاحات التكتيكية التي تحقَّقت خلال فترة "الذروة" في عام 2007 عندما طُبِّقت "خلايا الانصهار المشتركة" لهذه التقنيات "لتحديد الموقع، واستهداف، وقتل الأفراد الرئيسيين" ضِمن المنظَّمات الإرهابية، وخلايا المتمردين والميليشيات الشيعية.

وتركِّز الأساليب القائمة على أساس السكان على مكافحة التمرد والجهود المركزة لمكافحة الإرهاب التي تَضع "عمليات الهوية" في مركز الجهود "للتحديد الإيجابي، وتتبُّع، وتَوصيف، ومنعِ عناصر التهديد". كما تمَّ استخدامُ أساليب الاستهداف القائمة على نظام تحليل الشبكات الاجتماعية SNA في مقابل الأساليب التي تعتمد على الأفراد ذوي المستويات العليا، وذلك ضدَّ شبكات الدعم (التمويل، التجنيد، التدريب، الأعمال اللوجستية، الإعلام، توجيه الأوامر، الإدارة) وذلك خلال دعْم الأنشطة غير الحركية مثل: توزيع المنشورات، ومُلصقات "المطلوبين أمنيًّا" وحملات رسائل الجوال القصيرة، والخطوط الساخنة، التي تستخدم جميعًا لخَلْق "تركيز بقعة الضوء" ضد بعض عناصر التهديد المحددة.

منذ انتهاء العمليات القتالية في العراق وأفغانستان، نَضَجتْ نظرية الشبكة الاجتماعية بشكلٍ أكبر لتتحوَّل إلى عنصر أساسيٍّ في التَّفكير المنهجيِّ، وهو ما يبدو واضحًا في الإصدارات الأخيرة (للدليل الميداني لعمليات الجيش)، والإصدار المنهجيُّ الجديد للتحليل الاستخباراتيُّ، والاستخبارات المشتركة

لإعداد البيئة التَّطبيقية، والدليل الميداني للجيش فيما يَتعلَّق بالاستهداف، وذلك من بين مصادر أخرى، وقد أصبحت تقنيات نظام تحليل الشبكات الاجتماعية SNA أيضًا جزءًا من برامج التدريب المؤسسية للجيش، التي ستَظلُّ تُناقَش على نِطاق واسع في الأدبيَّات المهنيَّة المتعلِّقة بسير الحرب غير النظامية والمختلطة، ومكافحة الإرهاب، وعمليات دَعْم الاستقرار.

على مدى العقد الماضي، أصبحت تقنيات تحليل الشبكات الاجتماعية SNA أكثر اندماجًا في العملية التطبيقيَّة للاستهداف؛ فقد قامت الخدمات العسكرية (بشكل أساسيٍّ في الجيش وسلاح مشاة البحرية) بتطوير أساليب رسمية تتعلَّق بـ"عمليات الهوية".

ويمكن القول: إن سلاح مشاة البحرية يميلون أكثر إلى إضفاء الطابَع المؤسسيِّ لتحويل هذه الدروس العملية إلى مبادئ منهجية، وتركِّز هذه الاستراتيجية على تحديد الأفراد والشبكات التي تسعى إلى عرقلة العمليات، في الوقت الذي يتم فيه تَزويد القادة المخططون بالمعلومات الحديثة "في الوقت الحقيقيِّ" لتحديد الهُويَّة، والانتماءات، والتفويضات الخاصة بالفرد المعنيِّ، للربط بين الأشخاص، والأماكن والأحداث بأسلوب علميٍّ، وتجنُّبِ عدم الكشف عن الهُوية وحرية الحركة، أَدْرج سلاحُ مُشاة البحرية هذه "الاستراتيجيات القائمة على الهوية" عبر ستِّ مراحلَ لتخطيط بناء الحملات المشتركة، مما يعكس الحاجة إلى جمع واستغلال، وتحليل هذه الأساليب في وقت مُبكِّر من العمليات، للحدِّ من عدم الكشف عن هُويَّة العناصر الخطرة، وقد تمَّ تقنينُ هذا المفهوم مؤخرًا في استراتيجية عام 2020 لدى مركز عمليات الهوية الخاص بسلاح مشاة البحرية التابعة للولايات المتحدة (IdOps)، وهي الاستراتيجية التي قدَّمت رؤية شاملة ونهجًا لتطوير (مركز عمليات الهوية الخاص بسلاح مشاة البحرية التابعة للولايات المتحدة) عبر مجموعة من العمليات العسكرية.

وقد أدرجت وزارة الدفاع مؤخرًا مفهوم "استخبارات الهوية" (I2) ضمن المنهجية المشتركة، وكذلك تحسين منهجية الاستهداف القائم على الشخصية، حيث لا يعتبر مفهوم استخبارات الهوية (I2) عملية استخباراتية في حد ذاتها، وإنما نتاج تحليليّ مُفصّل مُستمد من اندماج سمات الهوية المختلفة (البيولوجية والجغرافية والسلوكية، والمعلومات المتعلقة بالسُمعة) في عملية التخطيط التطبيقيّ. حيث يعمل مفهوم استخبارات الهوية (I2) على دمج عدة مجالات تطبيقية وفنية مختلفة، بما في ذلك القياسات البيومترية المخابراتية (BEI)، ومعلومات الطب الشرعي المتعلقة بالاستخبارات، واستغلال الوثائق والبيانات الإعلامية المتاحة، وغيرها من كافة مصادر المعلومات، بغرض "ربط الأفراد مع غيرهم من الأشخاص والأماكن والأحداث، أو المواد" وتحليل أنماط الحياة، ويُحدِّد هذا المنهج الجديد دورًا رئيسًا لمفهوم استخبارات الهوية (I2) عبر مجموعة واسعة من المجالات المهمة لتمييز وتحديد بعض الفاعلين المحددين في أرض المعركة، ويشمل ذلك بعضَ المهام مثل الهجمات المركزة، نقاط التفتيش، وعمليات الأمن المحليِّ، ومراقبة الحدود والدفاع البحريِّ وحماية القوات، ودَعْم تنفيذ القانون في الدولة المضيفة، وغير ذلك من المهام التحليلية التي تتطلَّب رسْم الخرائط التفصيلية "لتضاريس العناصر البشرية".

وباختصار، فإنَّ التحديات الأمنية في العِقد الماضي سلَّطتِ الضوءَ بوضوح على الأهمية المتزايدة للهُوية في ساحة المعركة الحديثة، وقد ظهر ذلك في تطوُّر عمليات استهداف ومكافحة الإرهاب، وكذلك خلال حملات مكافحة التمرد ضد القوات غير النظامية القادرة على الاندماج مع السكان المحليين، وإخفاء هُويَّتها من أجل كسب مَيزة لها على أرض الواقع، يُمثِّل هذا النمطُ من القتال اختلافًا كبيرًا عن منهجيات حروب الحِقبة الصناعيَّة مع التركيز على المناورات واسعة النِّطاق، وقوة الذخيرة، واستخدام القوة التقليدية، وقد انعكس هذا التغيير على أدوات الأسلوب المنهجيِّ الجديد؛ مثل نظام تحليل الشبكات الاجتماعية، ومركِّز عمليات الهُوية الخاص بسلاح مشاة البحرية التابعة للولايات المتحدة (IdOps) في عملية التخطيط وتحديد الأهداف.

وقد تم تصميم المنهجيات الجديدة للحرب الإلكترونية خصيصا لمواجهة التحدي المتمثل في مكافحة شبكات العدو، والمتطلبات التحليلية لعمليات الاستهداف المنقَّحة التي تُركِّز على المقاتل الفردي، وهو عنصر يتميَّز بأعلى قدر من الخصوصية في ساحات المعركة، كما يقوم القسم القادم بتسليط الضوء على هذه الأساليب التي لن تكون متاحة؛ بدون التطور المتزامن للعديد من التقنيات الرئيسة التي مكَّنت قواتِ الولايات المتحدة الأمريكية من جَمْع وتحليل كميات كبيرة من المعلومات الخاصة بالهُوية لفحص واستهداف المقاتلين الفرديين.



يعتمد تفعيل منهجيات الحروب على التطور المتزامن للعديد من التقنيات المؤثرة المتَّبَعة، وكثير منها لم يستخدم في ساحة المعركة قبل أحداث الحادي عشر من سبتمبر 11/9، حيث إن مثل هذه الابتكارات الخاصة بعمليات الرقابة المستمرة، ومواجهة الهجمات المحددة، وآليات توقُّع القياسات الحيوية وعوامل الطب الشرعيِّ الاستطلاعيِّ، وأدوات إدارة التحليل والمعلومات المتقدمة المصممة لتبادل بيانات الهُوية عبر جهاز الأمن القوميِّ، وقد ساعدتْ هذه التقنيات على خَلْق قاعدة معلوماتية حول حملة مطاردة المطلوبين ذوي الميول الإجرامية، وهي الحملة التي تَشُنُّها القواتُ الأمريكية ضد خصوم الشبكات والمقاتلين الفرديين.

وقد تم اعتماد التقنيات المتطوِّرة لخوض الحرب إلى حدٍّ كبير بما يتَّفِق مع الحلقات السابقة من عمليات الابتكار العسكري، الأمر الذي يحدِّد التوجه الأمريكي الهائل نحو اتباع المنهجيات الفنية والعلمية الاستراتيجية، ويمكن إرجاع أسلوب التتبع الفكريِّ للحرب إلى المفاهيم التي شكَّلها عِلمُ الشبكات في حِقبة ما بعد الحرب العالمية الثانية، والجهود المبذولة لتطبيق الهندسة والتقنيات المتقدمة في الرياضيات تُجاه المشاكل الأمنية الوطنية، هذا وقد قدَّم عِلم الشبكات التفكير التأسيسي للتطورات اللاحقة في النظريات القتالية، مثل شبكة الحرب المركزية، ثورة تقنيات الشؤون العسكرية (RMA)، والعمليات الفعَّالة، وقد تم استخدام البيانات الكمية والتحليلات المتقدمة لدعم الدقة في الموضوع الثابت بين تطوُّر هذه النظريات القتالية، والموضحة في صعود الحرب الإلكترونية.

قد أثَّر ذلك أيضًا على التفكير المماثل لتجرِبة أميركا الأخيرة خلال شنِّ الحملات العسكرية لمكافحة التمرد في فيتنام، مع تطبيق الأدوات العلمية والأساليب الكمية، التي فشلت في نهاية المطاف في تحقيق النتائج الاستراتيجية المرجوَّة، وفي خضمِّ هذا الفشلِ، قد تَنبأَ الجنرال وليام ويستمورلاند وغيره بساحات المعارك العسكرية المستقبلية بقوله:

"ستُكون مقرَّات قواتِ العدوِّ، والاستهدافُ الفوريُّ قَريبًا؛ وذلك مِن خلال استخدام وصلاتِ البَيانات، بمساعدة أجهزة الحساب الآلي الخاصة بتقييم الاستخبارات، و... مع أجهزة المراقبة التي يُمكِن لها تتبُّع العدوِّ باستمرار"

وتُعَدُّ تغذيةُ مِثل هذه الأفكار جزءًا كبيرًا من أسلوب الابتكار العسكري خلال عام 1970م و1980م، الذي يركِّز على خَلْق ثورة دقيقة مع التكنولوجيات المتقدمة في مجالات الاستطلاع والمراقبة، والقدرة على تحديد الهدف، ومع ذلك، وجِّهتْ هذه الثورةُ في المقام الأول إلى التحديات التنفيذية لساحة المعركة خلال الحرب الباردة وانخراط القوة التقليدية، وتسعى هذه الجهود إلى تأكيد آليات المراقبة الخاصة بالجنرال وليام ديبوي، أول قائد تدريب للجيش، التي تحثُّ على أن "ما يُمكن أن ننظر إليه، يمكن أن نَصِل إليه، وما يمكن أن نصل إليه، يمكننا قَتْلُه".

وأسهمتِ العديد من الأدوات التي تم تطويرها خلال هذه الفترة من الابتكار التقني بنتائج مذهلة خلال حرب الخليج الأولى، وقد تم تطبيقها مرة أخرى كجزء من النَّهج الأَوْليِّ للعمليات في أفغانستان والعراق على أساس افتراض أن حملات "الاستئصال الجراحيِّ" ستكون لها نتائجُ استراتيجية مماثلة دون الحاجة إلى تشكيلات برية واسعة واحتلال عسكريٍّ مطوّل، ومع ذلك، في كلتا الحملتين، فإنه سرعان ما اتَّضح أن ظهورَ نوع جديد من الخصوم سيتطلب مجموعة جديدة من الأدوات والأساليب، التي تلائم تحليل واستهداف الشبكات والمقاتلين غير النظاميين.

كما شهد هذا الإدراك بداية عملية للتكيف مع جيل من الأدوات والتقنيات القديمة التي صُمِّمت من أجل حِقبة الحرب الباردة الخاصة بمطالب جديدة لمكافحة الخلايا الصغيرة والمقاتلين الفرديين، وشمل ذلك تطويع أغراض أخرى للتكنولوجيات القائمة للمهام الجديدة، فضلًا عن دمج قدرات متطورة مثل الطائرات بدون طيار، وآليات القياس البيولوجيّ، والطب الشرعي الاستطلاعي في الاستخدام العملي، كان ذلك بالتأكيد هو الأكثر وضوحًا من بين هذه الأدوات وهو استخدام المركبات الجوية غير المأهولة، أو الطائرات بدون طيار، قبل 11/9، كان الاستخدام العملي محدودًا في المقام الأول إلى المهام الاستطلاعية في منطقة البلقان وأفغانستان؛ حيث لم يتمَّ اختبار هذه الآليات بنجاح كمنصَّات صالحة لحمل الأسلحة حتى أوائل عام 2001، ثم تمَّ تكييفه بسرعة للاستهداف الحركيِّ في أفغانستان.

وفي بداية الحملة العسكرية، دعا الجنرال تومي فرانكس طائرات البريداتور بأنها "آليات الاستشعار الأكثر قدرة في مطاردة وقتل عناصر تنظيم القاعدة وقيادات جماعة طالبان"؛ حيث ازداد المخزون من هذه الأنظمة الأساسية بمعدل 40 ضعفًا فيما بين عاميْ 2002 و2010، مع التوسع الكبير في استخدامها في العمليات العسكرية الفعلية؛ على سبيل المثال، خلال عام 2007، كان هناك مجموعة من 74 غارة عسكرية بطائرات بدون طيار في أفغانستان؛ ومع ذلك، بحلول عام 2012، بلغ متوسط هذا العدد 33 هدفًا في الشهر، ومع مرور الوقت تمكنت القوات باستخدام مزيج من تحسين أجهزة الاستشعار وحزم البرمجيات التحليلية من "إدراك وتصنيف الأشخاص والأشياء يدوية الصنع" والتوفير غير المسبوق لآليات (مراقبة الوقت الحقيقيِّ) من أجل تعقُّب المقاتلين الفرديين.

وربما استهدفت الغارات بطائرات بدون طيار "لقد انتقلنا من الندرة النسبية للممارسة الشائعة نسبيًّا" كجزء من استراتيجية الولايات المتحدة لمكافحة الإرهاب. كان المثال الأول من هذا هو هجمات طائرات بريداتور 2001 الذي قُتل فيه محمد عاطف، وهو عضو بارز في القاعدة على علاقة بتفجيرات السفارة الأمريكية عام 1998 في تنزانيا وكينيا، ومنذ ذلك الحين، أصبحت هذه الهجمات التكتيكية

الرئيسة تستخدم ضد تنظيم القاعدة وحركة طالبان، والجماعات التابعة لها في باكستان منذ عام 2007، وفي اليمن منذ عام 2009، وفي الصومال منذ عام 2006، وتشير التقديرات غير المصنفة إلى أن أكثر من 98 في المئة خارج ساحة الحرب استهدفت عمليات القتال الذي قامت به الولايات المتحدة على مدى العقد الماضي، وتم طرحها من خلال هذه الأنظمة الأساسية.

بينما حرب الطائرات بدون طيار قد استولت على حصة الأسد من اهتمام الرأي العام، حيث يمكن القول: إن تفعيل القياسات البيولوجية والطب الشرعي الاستطلاعي يوفِّر مظاهر أكثر وضوحًا للكيفية التي تطورت بها اتجاهات التكنولوجيا في دعم الحرب الفردية والاستهداف على أساس الهوية، ظهرت هذه الابتكارات مباشرة من خلال التحديات التنفيذية لمكافحة التمرد والحاجة إلى تحديد وتمييز الأعداء من السكان المحليين؛ حيث أدَّى هذا الأسلوب إلى التطور السريع واستخدام نُظم التحقق من الهُويَّة التكتيكية في ميدان القتال في كل من العراق وأفغانستان.

كما هو الحال مع تكنولوجيا الطائرات بدون طيار، لم يكن هناك أيُّ استخدام عملي كبير للقياسات البيولوجية من قبل القوات الأمريكية قبل 11/9، حيث بدأ برنامج التطوير البيومتري "تطوير القياسات الحيوية" للجيش فقط في عام 1999 في مختبر القيادة، وبحلول عام 2001 تم إنتاج الإصدار الأول من مجموعة أدوات القياس الحيوي الآلي (BAT)، ونظام جَمْع بصمات الأصابع وقزحية العين، والتخزين البيومتري وتحديد المعلومات الشخصية، وتم اختبار التكنولوجيا ميدانيًّا في البداية في منطقة البلقان لتحديد وتتبُّع دخول العمال الوطنيين المحليين إلى منشآت الولايات المتحدة، ومع ذلك، بعد وقت قصير من بَدء العمليات القتالية في أفغانستان والعراق، اعترَف المخططون العسكريون بحاجتهم الملِحَّة إلى أدوات إدارة الهُوية في ساحة المعركة؛ نظرًا إلى التحديات التنفيذية المبكرة، حيث أدركتْ وزارة الدفاع بسرعة التعرف على بيانات الهوية "على أنها القدرة القتالية الأساسية، وخصوصًا عندما تُقاتل الأعداء المسلحين الذين يختبئون بين السكان المدنيين".

وقد تم إدخال نموذج BAT إلى القيادة المشتركة للعمليات الخاصة في أفغانستان في أوائل عام 2002 لتسجيل الأشخاص المثيرين للارتياب، وبحلول عام 2003، تم استخدام هذا النموذج في العراق أيضًا، لأول مرة في معتقل أبو غريب لإدارة المعتقل، ومن أجل ربط تقارير استجواب المعتقلين البيومترية صدر BAT أيضًا في وحدات مشاة البحرية؛ حيث استخدم خلال إعادة التوطين من مدينة الفلوجة بعد العمليات القتالية الرئيسة في عام 2004. وكذلك في عمليات إدخال سكان المدينة؛ حيث إن القوات الأمريكية قامت بفرزهم والتسجيل البيومتري لجميع الذكور.

كما قامت بعمليات جَمْع الأسماء وتواريخ الميلاد، وأماكن الولادة والانتماءات الدينية، وغيرها من بيانات الطول والوزن ولون الشعر والعينين، وبصمات الأصابع ومسح القزحية، والصور الرقمية المختلفة، وتمَّت مقارنة هذه البيانات في مقابل هُويَّات المسلحين المعروفين والمشتبه بهم، وتم ربْط بطاقات الهُوية التي كانت تستخدم لمراقبة تدفُّق السكان الذكور داخل وخارج المدينة، وقد أظهر الحادث المنفصل في نفس الشهر في مدينة الموصل؛ الحاجة الملِحَّة للتحقق وتتبُّع الهويات في ساحة المعركة بشكل صارم، بعد تفجير منشأة عسكرية لتناول الطعام من قِبل متمرِّدين ينتمون إلى تنظيم القاعدة، مما أَسفَر عن مقتل 22 شخصًا، حيث أصبحت أدوات إدارة الهوية بعد ذلك ضرورة تنفيذية في البيئة، حيث يتنقل العدو المجهول بحرية خارج البوابات.

وقد توسَّع الاستخدام العملي للقياسات الحيوية بسرعة؛ فقد اتجهتِ الولايات المتحدة نحو استراتيجية مكافحة التمرُّد، وأصبح السكان المتمركزون في العراق هم الأداة الحاسمة، كما نمَّتْ قاعدة بيانات الهوية مع مرور الوقت، القياساتِ الحيويَّة، وارتبطت مع الطب الشرعي التنفيذي، واستُخدِمت على نطاق واسع لتحليل واختراق الخلايا التي تستخدم العبوات الناسفة ضد قوات التحالف.

على سبيل المثال، خلال 2007-08، ارتبط أكثر من 1700 فردٍ بأدلة الطب الشرعي المتعلقة بتصنيع واستخدام هذه الأسلحة ضد قوات التحالف، وفي العام نفسه كشفتِ المعلومات الواردة في قواعد البيانات البيومترية؛ أن العديد من الموظفين العراقيين المتقدمين للاختيار إلى أكاديمية الشرطة العراقية قد تطابقت هوياتهم مع الإرهابيين المحتجزين سابقا والمتمردين المشتبه فيهم، وحتى العديد من الأفراد اصحاب السجلات الجنائية في الولايات المتحدة بحلول عام 2011، وفي نهاية العمليات العسكرية في العراق، قامت الولايات المتحدة بتجميع قاعدة البيانات البيومترية التي تحتوي على حوالي ثلاثة ملايين من ملفات المواطنين العراقيين.

وبالمثل في أفغانستان، تم تفعيل أكثر من 7.000 جهاز جمع بيومتري لدعم عمليات الاعتقال، وتنفيذ الأوامر ذات المخاطر العالية، واستهداف الغارات ضد المتمردين فيما بين عامي 2004 و2011 استخدمت القوات الأمريكية 1.6 مليون من المسجلين على أكثر من 1.1 مليون شخص - أي ما يعادل تقريبًا واحدًا من كل ستة من الذكور في سن القتال، وتستخدم هذه البيانات لتحديد أكثر من 3000 عدو مقاتل بشكل إيجابي، وكانت هذه القدرة لها أهمية خاصة في أفغانستان، البلد ذات محدودية القدرات المؤسسية للتحقق من الهوية التي لديها فقط بضع شهادات ميلاد، ورخص القيادة، أو وثائق المواطنة، وقد تفاقم هذا الوضع من خلال السوق السوداء النشطة التي تعمل في مجال تزوير وثائق الهوية.

يستهدف إدماج أساليب BEI الحد من قدرات قيادات التمرد على الاختفاء بين السكان المحليين، ويعمل التحالف والقوات الأفغانية أيضًا بانتظام مع قوائم المراقبة البيولوجية ورسائل" التحذير" التي أدَّت إلى أوامر"الاعتقالات، وإزالة عدم الكشف عن هوية المتمردين"، وبحلول نهاية العمليات القتالية النشطة في أفغانستان، كانت الولايات المتحدة قد وضعت حوالي 33.000 من هُويَّات الأفراد على المقاييس الحيوية من أجل تفعيل قائمة المراقبة، وهناك مثال حي يدل على قوة هذه المعلومات في عام 2011 بعد

هروب نحو 500 من سجناء طالبان من سجن قندهار ساربوسا. وكان جميع المعتقلين قد خضعوا سابقًا إلى عمليات التسجيل البيومتري، وفي غضون شهر، أعيد القبض على نحو 30 فردًا فقط نتيجة للضوابط البيومترية العشوائية في المنطقة المحلية.

وكانت إحدى نتائج جمع البيانات البيومترية واسعة النطاق في ساحة المعركة، وهي تحسين القدرة على مراقبة هويات المقاتلين وتتبع حالات ارتداد القتال، وكانت تقديرات معدلات الارتداد متغيرة إلى حد ما بسبب التحدي المتمثِّل في التحقق والتصنيف، وكيف يتم تعريف مصطلح "إعادة الاشتباك"، ومع ذلك هناك اعتراف عام بأن بعض المعتقلين المفرَج عنهم قد عادوا إلى القتال الفعلي، على سبيل المثال، في نهاية العمليات القتالية الأميركية في العراق، تم كشف ما يقرب من 10 في المئة من جميع البيانات البيومترية التي تربِط الطب الشرعي بمواد المتفجرات ووجود علاقة مع الأفراد الذين تم إطلاق صراحهم مسبقا من الاحتجاز.

وفي الآونة الأخيرة، قد عاد أبو بكر البغدادي أمير" الدولة الإسلامية "الأكثر شهرة، وكان قد تم القبض عليه في الأصل من قبل قوات الولايات المتحدة في عام 2004 بالقرب من الفلوجة، وقضى بعض الوقت في منشأة الاعتقال الأمريكية في مخيمات بوكا وآدر قبل إطلاق سراحه بشكل منفصل، أشار تقرير الحكومة العراقية مؤخرًا إلى أن نحو 17 من 25 من قادة الدولة الإسلامية الأهم قد قضوا بعض الوقت في معتقلات الولايات المتحدة فيما بين عامي 2004 و2011 وعرضت التقنيات البيومترية عددًا قليلًا من الوسائل الفعالة لتتبُّع هذا الارتداد ومراقبة تدفُّق المقاتلين الأجانب من خلال مناطق الصراع.

ومنذ بَدء العمل في العراق وأفغانستان، انتشرت تقنيات التحقق من الهوية إلى المناطق الأخرى مع التحديات التنفيذية المماثلة من التحقق من الهوية، مثل عمليات مكافحة القرصنة في شرق أفريقيا، كما أوضَح المتخصص في استخبارات الهوية في تدريب الجيش والقيادة "القياسات الحيوية موحدة بالنسبة إلى

العدو" ويمكن تحديد العناصر الفاعلة حتى في غياب ملفات التعريف على أساس الحالة القياسية، وفيما يخصُّ الاعتراف بالقيمة التنفيذية لهذه التكنولوجيا، فقد وجهت وزارة الدفاع مؤخرًا أوامر لدمج القياسات الحيوية في التخطيط للبعثات العسكرية، وعلى وجه الخصوص واصل الجيش الأمريكي الضغط من أجل تكامل العديد من الأساليب الجديدة، كان آخرها تطوير بيانات استغلال القياسات الحيوية الصوتية (VIBES) وهي أداة لتحديد المواجهة، وتتبع الأفراد ذوي الأهمية القتالية المرتفعة، وتمكين شبكة المعلومات البيومترية من تحليل الارتباط، وهناك أيضًا جهود أخرى مثل تطوير إصدارات أحدث الأجهزة المحمولة يدويًّا لجمع البيانات البيومترية، وكذلك الترقية الجارية لقاعدة البيانات الآلية البيومترية لنظام تحديد الهوية (ABIS) لإدارة وتبادل البيانات البيومترية في الحكومة.

الطب الشرعي الاستطلاعي هو مجال آخر؛ حيث تتطور التكنولوجيا العسكرية الجديدة بسرعة في الاستجابة للمطالب التنفيذية لشن الحرب، على مدى العقد الماضي، كانت أدوات وتحليل الطب الشرعي المركزي تدلُّ على أساليب استهداف وتحديد العناصر الفاعلة، وربط الناس، الأماكن، والأشياء، والنوايا والأنشطة والمنظمات والفعاليات بكل عملية، وفي أواخر عام2004، كانت قوات الولايات المتحدة في العراق رائدة في استخدام الطب الشرعي الاستطلاعي لتحديد صانعي العبوات الناسفة والشبكات، بدأ مركز المخابرات البرية القومية في توسيع القدرات الموجودة للجمع بين خلايا المتفجرات، ويركِّز في المقام الأول على تحليل المعلومات الاستخباراتية والتقنية الكيميائية للأسلحة.

كان وجود هذه المختبرات سببًا في الزيادة الكبيرة في القدرات النوعية والكمية لقوات الولايات المتحدة وإدراكها والحفاظ عليها، وتحليل مواد الطب الشرعي في مسرح العمليات ودعم طرق التعرف على الهوية ضد شبكات المتمردين. وبحلول عام 2006، تم تفعيل هذه المنشآت في كلٍّ من العراق وأفغانستان، بما في ذلك قدرات جديدة للذخيرة والملابس، وبصمات الأصابع الخفية، وتحليل الحمض الديوكسي ريبونوكلييك (DNA) وكذلك الطب الشرعي الرقمي، وبحلول عام 2010، نشرت الولايات المتحدة

سبعة مجموعات من هذه المختبرات الاستطلاعية بالعراق وثمانية في أفغانستان، وخلال ذلك العام وحده، تم تفعيل عمليات الاستهداف والقبض على أكثر من 700 شخص ذوي ارتباط بشبكات تصنيع العبوات الناسفة والإرهابيين المشتبه بهم، والعناصر الفاعلة الإجرامية الأخرى.

ولا سيما في حالة تحليل الحمض النووي، إلا أنه قبل العمليات العسكرية في العراق وأفغانستان كان الاستخدام العملي محدودًا جدًّا من هذه التقنية خارج دورها التقليدي في دعم التحقيقات الجنائية، على الرغم من تلك الدقة العالية، فإن التقنيات الحالية لتحليل الحمض النووي تُعدُّ بطيئة ومكلِّفة؛ لذلك تقتصر عادة على استخدام الفحص المخبريّ، وقد تغيَّر هذا الوضع بشكل كبير خلال العقد الماضي، مع تركيز جهود الجيش لدعم هذه القدرات إلى المختبرات المتنقلة التي تعمل على الدعم المباشر من قادة العمليات، وكانت البداية في العمليات العسكرية في العراق، وقد استُخدِمت في المقام الأول في مهامِّ الطب الشرعي الجنائي للتحقيق في عمليات القتل خارج إطار القضاء، ولكن مع مرور الوقت توسَّعت المهمة لتحليل العينات المستخرَجة من مقرَّات التعذيب والمخابئ الإرهابية، وتحديد هُوية الأفراد ذوي الأهمية المرتفعة الذين قُتلوا أو اعتُقِلوا خلال تلك المداهمات.

وبحلول عام 2008، ذكَرت القوات العسكرية الأمريكية القيام بجمع نحو 80.000 عينة من الحمض النووي الفردي لدعم متطلبات تطبيق القانون والاستخبارات العسكرية، وبحلول ذلك الوقت، كانت المختبرات الاستطلاعية قادرة على معالجة العينات ذات الأولوية العالية في أقل من 24 ساعة، وربما جاء تطبيقها الأكثر شهرة عندما حلَّل مختبر الطب الشرعي التابع للجيش الأمريكي في أفغانستان الحمض النووي من جثة أسامة بن لادن لتأكيد هُويَّته بعد وقت قصير من الغارة التي شنَّتها القوات البحرية والبرية والجوية الأمريكية، في شهر مايو من عام 2011

وفي الآونة الأخيرة، فإن عمليات القوات الأمريكية الخاصة قامت باختبار قراءة الحمض النووي الاستطلاعيّ في المواقع الأمامية، وذلك باستخدام الأجهزة التجارية التي تَزِن حوالي 60 رطلًا، وحقَّقت النتائج المرجوّة في أقل من 90 دقيقة تحسنًا كبيرًا خلال التكنولوجيات المتاحة قبل بضع سنوات.

وعلى مدى العقد الماضي أصبحت التكنولوجيات الناشئة تدعم تحليل الطب الشرعي للأدلة القائمة على استهداف النهج المستخدم كجزء من استراتيجيات مكافحة الإرهاب ومكافحة التمرد، وكذلك المساهمة في عمليات الاستقرار، والحكم المحليِّ، وإعادة تأسيس حكم القانون، وخلال الفترة الانتقالية من العمليات القتالية في العراق وأفغانستان أصبح نظام العدالة الجنائية الأصليّ هو الوسيلة الوحيدة لإبعاد المتمردين والإرهابيين من أرض المعركة، وأصبح الطب الشرعي هو الأداة الرئيسة التي تُمكِّن القوات الأمريكية من تحديد الموضوعات ذات الاهتمام بدقة، وتوفير المعلومات المتعلقة بالأنشطة الإجرامية والإرهابية، بطريقة تتَّفق مع معايير الإثبات المعترف بها.

فعلى سبيل المثال، خلال عام 2012، قدَّمت قوات الولايات المتحدة تحليل الأدلة الجنائية لدعم نحو 120 من القضايا المعروضة على المحاكم الأفغانية التي تربط بين المقاتلين الأعداء من خلال بصمات الأصابع الخفية وأدلة الحمض النووي، مما أسْفر عن معدل إدانة 97 في المئة من هذه الحالات، من الناحية العملية، فهذا يعني أيضًا أن عمليات الاستهداف في كثير من الأحيان كانت مصمَّمة لغرض محدد للحصول على أدلَّة مادية لدعم الإجراءات الجنائية والإدانة بموجب قواعد القانون المدني.

وأشارت إحدى الدراسات حول استخدام الطب الشرعي والقياسات الحيوية خلال هذه الحملات وكيف يمكن لهذه التقنيات أن تقدِّم دعمًا مباشرًا دقيقًا لتشكيل البيئة التنفيذية، بما في ذلك حَظْر سلسلة التوريد، وعمليات تمويل التهديد المضاد، عمليات المعلومات، وتدمير المخابئ، واعتقال الأفراد ذوي الأهمية العالية.

وعلى سبيل المثال، قدَّرت فرقة العمل الأمريكية المسؤولة عن عمليات الاعتقال في أفغانستان أن نحو 70 في المئة من الأهداف الفردية على أرض المعركة، تم تحديدها بمساعدة القياسات الحيوية وتقنيات الطب الشرعي، وخَلُصت دراسة مكتب الرقابة الحكوميّ الأمريكي إلى أن الصراعات في العراق وأفغانستان قد أحدثت ثورة على مستوى الطب الشرعي الاستطلاعي، وتحديدًا في استخدام البصمات الخفية، وتحليل الحمض النَّووي لدعم العمليات العسكرية.

إنَّ النموَّ السريع للقياسات الحيوية، وآليات الطب الشرعي، والكميات الهائلة من البيانات الواردة من منصَّات المراقبة المستمرة، قد خلق تحدِّيًا جديدًا للمحلِّلين على وجه التحديد في مهمة الفحص، من خلال قدرٍ لم يُسبَق له مثيل من المعلومات التي تم جَمعُها على المستوى التكتيكي؛ وفْقًا لتقرير واحد، فإن هذا الطوفان من بيانات الاستشعار جعل من المستحيل تتبُّع وتحديدَ الأنشطة المشبوهة والتهديدات الأمنية المحتملة فقط من خلال العمليات التحليلية البشرية.

حيث كانت هناك مشكلة تتعلَّق بمجال تجهيز وربْط تيارات متعدِّدة من البيانات غير المهيكلة؛ مثل :التقارير الدورية وأرقام الهواتف الخلوية، وبيانات السيرة الذاتية، وملفات الوسائط، وملفات الهوية البيومترية، والأدلة الجنائية، وقد جعلت ضخامة هذا التحدي عمليةَ إدارة المعلومات مهمة حاسمة، لها دور مُتفرِّد في شنِّ الحروب العسكرية؛ ولهذا السبب، أصبح تطويرُ أدوات وأساليب تنظيم وتخزين وتحليل ونَشْر هذه البيانات الجديدة مهمة كبرى، إذ يتم التقدير كما يَنْبغي في تحقيق الابتكار التقني العسكري على مدى العقد الماضي.

كما بدأت القوات الأمريكية في جمعِ كميات كبيرة من البيانات البيومترية في ساحة المعركة، وكانت هناك حاجة ملحَّة إلى قاعدة بيانات موثوقة لمعالجة وتخزين ومطابقة النتائج البيومترية، وشَمِلت القدرة على تبادل المعلومات الخاصة بالهُوية بين القوات التكتيكية المشتَّتة على نِطاق واسع، وكذلك بين عناصر وزارة الدفاع الأخرى، وأجهزة الاستخبارات، وتطبيق القانون المحلي، وأدَّى ذلك إلى تصميم النموذج الأولي في

عام 2004 حول لماذا ستصبح في نهاية المطاف أنظمة ABIS متعدد الوسائط البيومترية المركزي هي مخزن البيانات العسكرية، القادرة على معالجة وتخزين وإنتاج نتائج بصمات الأصابع، ومسح قزحية العين، ومسح الوجه للأشخاص مثيري الارتياب، وقد تم تصميم هذا النظام لدعم مجموعة متنوعة من المهام التنفيذية، بما في ذلك عمليات الاعتقال وفحص مكافحة الإرهاب والعمليات الخاصة، ومتطلبات الاستخبارات الأخرى، والأهم من ذلك، القدرة على تبادل البيانات مع وزارات الدفاع الأخرى، الوكالات والشركاء متعددة الجنسيات.

كما بدأت وزارة الدفاع في جَمع كميات هائلة من بيانات الهوية على أرض المعركة، كان هناك أيضًا حاجة إلى تحسين التجهيزات والقدرات التحليلية للفحص، من خلال تزايد بيانات ومنهجيات أسلوب SNA لدعم الاستهداف. وأدَّى ذلك إلى تكييف الأدوات التحليلية مثل مفكرة المحلل، كجزء من النظام الموزع المشترك، ومنصة بالانتير الجديرة بالاهتمام، التي تستخدمها الوحدات العسكرية في أفغانستان وأماكن أخرى، وقد استُخدِم نظام بالانتير لتحليل الشبكات، وتصور البيانات والاستناد إلى التطبيقات التجارية، التي وضعت أصلًا في شبكة Paypal بايبال؛ لاستخدامها ضد شبكات الجريمة الإلكترونية، وفي الكشف عن المعاملات المالية المزورة، كما تم استخدام البرنامج لتحليل أنماط الجريمة في المناطق الحضرية، ورسم الخرائط الموضِّحة لأنشطة عصابات المخدِّرات في المكسيك، وتفكيك شبكة التفجيرات الانتحارية السورية عن طريق تحليل مئات من سِجلات المنضمين لتنظيم القاعدة، التي استولت عليها قوات الولايات المتحدة الأمريكية في دولة العراق، مع الحاجة المتزايدة إلى تحديد المسار، واستهداف الأفراد عبر ساحة المعركة.

وقد وضعت الأدوات المتخصصة الأخرى التي تركِّز بشكل خاص على إدارة الهوية وارتباط السمات المشتركة، وقد تم تصميم هذا التطبيق من أجل جمع ونقل البيانات البيومترية، ووسائل الطب الشرعي في دعم اكتشاف وتحليل الهوية، داخل بنية النظام المشترك الموزع للجيش، ومكافحة التجسس، فإن تقارير

الاستخبارات البشرية ونظم الجمع تعتبر هي النظام الأساسي المصمم لإدارة وتحليل المعلومات الخاصة بالهوية المستمدة من التحقيقات وجمع بيانات الهوية، وعمليات الاستفادة من الوثائق، تُعَدُّ بيانات الهوية البيومترية البيولوجية بالاستخبارات في وزارة الدفاع هي أداة أخرى تسمح لخبراء الاستخبارات بتحليل المعلومات البيومترية ودمجها داخل منظومة ABIS، وتقديم هذه المعلومات إلى المستخدمين في هذا المجال يتضمَّن القدرة على الربط بين سمات الهوية والبيانات الظرفية، السياقية، والزمنية المرتبطة بأحداث الجمع البيومتري.

إن تطوُّر هذه الأنظمة على مدى العقد الماضي يُسلط الضوءَ على الأهمية المركزية لإدارة المعلومات وتحليل البيانات لشنِّ الحرب، في حين ركَّز في الأصل على التحقق من الهُوية وحماية القوات، ومع مرور الوقت تم تكييف هذه الأدوات البيومترية مع الدعم المباشر للاستهداف إلى أن تم إدماج هذه التكنولوجيات العسكرية والأساليب في المؤسسة الأمنية الوطنية العامة، ولا سيما مساهمتها في منهجيات الفحص على أساس الهوية، التي أصبحت عنصرًا رئيسًا في الطريقة التي يتم بها خوض الحرب في الداخل كما في الخارج.

وقد تم الجمع بين انتقال هذه الأدوات من أرض المعركة إلى الجبهة الداخلية مع التوسع غير المسبوق في تبادُل المعلومات بين المجتمعات العسكرية، والاستخبارات، وتطبيق القوانين المحلية؛ حيث يتم توضيح الجهود الحالية من أجل تتبُّع ورصْد المقاتلين الأجانب في سوريا، وتوضيح إلى أي مدى أصبحت الحكومة تُشارِك في عمليات الحرب الإلكترونية، التي تَعتمِد على تبادُل البيانات والتعاون العملي، والتكامل الفني في جهاز الأمن الوطني بأكمله.

وقد ركَّزت هذه الاستراتيجية في المقام الأول على الرصد والاعتقال، والتحقيق في التهديدات المحتملة للوطن، وعلى الأخصِّ من خلال فحصِ المسافرين الأجانب الذين يدخلون في نِطاق الرقابة الحدودية، ولكن أيضًا تحديد المتطرفين الذين يحتمل أن يكونوا ذات صِلة بالإرهاب الدولي، كما هو الحال مع

استهداف الجيش في العراق وأفغانستان، فعلى مدى العقد الماضي أصبحت تلك البرامج للأمن الداخلي تحركها المخابرات على نحو متزايد، وتعتمد على استخدام التكنولوجيات المتقدمة لإدارة المعلومات.

ويتكوَّن الخط الأول من الدفاع عن الوطن من مجموعة متنوعة من برامج فحص الهجرة الموجهة في المقام الأول إلى شبكات السفر ومنافذ الدخول، وقد أصبحت إدارة الهوية هي العنصر الرئيس لعملية الفحص على أساس المخاطر، بناء على المعلومات الجغرافية والشبكات البيومترية للمسافرين الأجانب، الذين يسعون إلى دُخول الولايات المتحدة. تُقام هذه المعلومات ضِمن شبكةٍ من قواعد البيانات القابلة للتفعيل المتبادَل، الذي يسمح إلى عملاء الحكومة بالتحديد البيوغرافي، البيومتري، وفي بعض الحالات، يمكنهم من الوصول إلى بيانات الحمض النووي، وهي البيانات التي تم إعدادها من قِبل وزارات العدل، والدفاع، وأجهزة الاستخبارات.

مِثالين من هذا النموذج هما الفحص على أساس الهُوية والنظام الإلكتروني لتصريح السفر (ESTA) وبرنامج مؤشر تكنولوجيا الزوار وحالة الهجرة (US-VISIT) ESTA وهو قاعدة بيانات قائم على أساس السير الذاتية المستخدمة لتحديد أهلية المسافرين بالإضافة إلى فَحْص المخاطر المحتملة من الرعايا الأجانب، قَبْل دخول الولايات المتحدة، ويَكتمِل ESTA بواسطة برنامج US-VISIT الذي يتضمَّن قواعد بيانات متعددة من السير الذاتية والبيولوجية المستخدمة للتحقق من الهُوية والاختيار عبر المسافرين ضد قوائم المراقبة على المستوى المحليِّ.

العديد من التقنيات والأساليب التي يتم تطبيقُها ضد تحديات أمن الوطن الجديدة؛ تطوَّرت بالتوازي مع تلك التقنيات المستخدمة في العراق وأفغانستان، وغالبًا ما تشترك في البيانات نفسها حول التهديدات المحتملة، وأحد الأمثلة البارزة على ذلك هو نظام التحقيق في المكتب الفيدرالي (FBI) وتحديد هوية الأجيال القادمة (NGI)، وقام مكتب التربية العربي مؤخرًا بتحديث التخزين البيومتري الذي يحتوي على أكثر من 100 مليون سجل بصمة وملفات حيوية أخرى.

ويشمل هذا النظام مشروعَ تعريف القدرة على البحث الجنائي، وكذلك المخطط المتكامل، مسح القزحية، الندوب، العلامات، والوشم، والبصمات الخفية في قاعدة البيانات الوطنية للبحث، وبالمثل تحافِظ وزارة الأمن الداخلي (DHS) على النظام الآلي الخاصة بها ونظام تحديد الهوية (IDENT)، وكذلك على مخزن البيانات البيومترية والبيوغرافية المستخدمة للأمن القومي، وإدارة إنفاذ القانون، ودائرة الهجرة، وإدارة الحدود؛ (IDENT) تَدعم متطلبات الأمن الوطنيّ من خلال توفير مَسْح قزحية العين وقدرات مطابقة الوجه للدوريات الحدودية في الولايات المتحدة وغيرها من الكِيانات.

ووَفْقًا للتقديرات الأخيرة، فإن IDENT تقوم بمعالجة حوالي 300.000 معاملة في اليوم، بالاعتماد على قاعدة بيانات مكونة من 173 مليون هوية فريدة، وترتبط قاعدة البيانات أيضًا مع القياسات الحيوية لدى حرس الحدود الأمريكي المرتبط ببرنامج النظام البحري الذي يتكوَّن مِن نُظُم التحقق من الهوية المنتشرة على 23 جهازًا يُستخدَم لتحديد المجهولين في البيئة البحرية، بما في ذلك الإرهابيين المشتبه بهم، والمشتبه فيهم جنائيًّا، وغيرهم من الأفراد مثيري الارتياب.

وقد ظهرت القوة التحليلية المستمدة من تكامُل البيانات بين الوكالات مؤخرًا، عندما أشار مكتب التحقيقات الفدرالي إلى إرهابِي الدولة الإسلامية الملثَّم المعروف باسم "جون الجهادي"، الذي ظهر في أشرطة الفيديو التي تصوِّر قَتْل العديد من الرهائن، بما في ذلك مواطنون أمريكيون، واستنادًا إلى بيانات الصورة والصوت، قد تعرَّف مكتبُ التحقيقات الاتحادي على الفرد بمساعدة من وزارة الدفاع وشركاء الاستخبارات الأجنبية، وأشار مساعد مدير مكتب التحقيقات الفدرالي إلى قسم خدمات معلومات العدالة الجنائية ما يلي:

مكتب التحقيقات الفدرالي لا يمكن أن يؤدِّي مهمته بنجاح إذا لم يكن لدينا إمكانية التفعيل المتداخل مع وزارة الأمن الوطني والعمل المشترك مع وزارة الدفاع؛ لأن لديهم المعلومات اللازمة في مخازن البيانات البيومترية، وهي بيانات غير متوافرة لدينا.

أيضًا يتم استخدام وزارة الخارجية والقنصليين في الخارج لأدوات القياس الحيوي المماثلة وقواعد بيانات السيرة الذاتية، مثل قاعدة البيانات القنصلية الموحدة (CCD) لفحْصِ جميع طالبي تأشيرات الولايات المتحدة، وفي عام 2001 بدأت CCD بتخزين الصور لجميع طالبي التأشيرات، ومنذ عام 2007 شملت 10 ملفات مَسْح بصمات الأصابع التي يمكن أن تكون مشارًا إليها ضد البيانات الواردة في وزارة الأمن الداخلي ومكتب التحقيقات الفدرالي، وأنظمة وزارة الدفاع.

ويقال: إن قاعدة البيانات هذه تحتوي على حوالى 143 مليون سجل من السير الذاتية لطلبات التأشيرات التي يعود تاريخها إلى منتصف عام 1990 كجزء من إجراءات التأشيرة، يُطلَب من الموظفين القنصليين التحققُ من خلفيات مقدِّم الطلب إلى القنصلية ونظام الدعم الذي يسرد الأفراد، وأولئك الذين حرموا في السابق من التأشيرات، تحتوي هذه القاعدة على 42.5 مليون سجل، ما يَقرب من 70٪ منها يأتي من وكالات أخرى، بما في ذلك وزارة الأمن الداخلي ومكتب التحقيقات الفدرالي، وإدارة مكافحة المخدرات.

تم تصميم كل من وحْدة الدفاع الرئيس، أجهزة الاستخبارات، وبرامج فَحْص الأمن الداخلي للاستفادة من معلومات الهُوية الواردة في قاعدة بيانات الفحص الإرهابي التي يحتفظ بها مركز الكشف عن الإرهابيين الخاص بمكتب التحقيقات الفدرالي (TSC) في السنوات الأولى 2 بعد افتتاحه في عام 2003، فيما وَرَد أن TSC أصدر حوالى 6000 تنبيه إلى أجهزة الأمن الأمريكية على أساس الهويات أو أشخاص يشتبه في صلاتهم الإرهابية بجهات أجنبية إرهابية معروفة، والتوسع الأخير في الهيكل يمكنه الآن أن يقوم بمراجعة تلقائية لجميع طالبي التأشيرات غير المهاجرين لتحديد أي روابط إرهابية محتملة واردة في بيئة هويات الإرهابيين (TIDE) وقواعد البيانات الوطنية الأخرى.

في بعض الحالات، قد يشمل أيضًا المعلومات التي تم الحصول عليها من الشركاء الأجانب من خلال اتفاقات مشاركة البيانات المتبادَلة المتعلِّقة بالبيانات المفقودة والمسروقة وجوازات السفر، بيانات الحجز والمعلومات البيومترية، وحتى الحمض النووي لتحديد احتمال وجود صِلة بين الإرهابيين المعروفين وزملائهم غير المعروفين.

تُعدُّ قاعدة البيانات منفصلة، ولكنها متكاملة فيما بينها، ويتم الاحتفاظ بها أيضًا من قِبل المركز القومي لمكافحة الإرهاب، وتشمل هذه البينات جميع المصادر والمعلومات السرية التي قدَّمها مكتب التحقيقات الفيدرالي، وأجهزة الاستخبارات، وعناصر وزارة الدفاع، وقد أصبحت بمثابة المعلومات القياسية الموحدة في البلاد للفحص والكشف عن الإرهابيين المعروفين والمشتبه بهم، وتُستخدَم مقتطفات من TIDE لتجميع قوائم المراقبة لمختلف برامج الأمن الداخلي بما في ذلك برنامج الطيران الآمن لإدارة أمن الطيران؛ حيث يتم فحص هويات الركاب من خلال الكشوف الصادرة من المطارات الأمريكية.

اعتبارًا من مطلع عام 2014 سجلت ملفات TIDE الواردة نحو 1.1 مليون شخص، ووَفْقًا للتقارير الصحفية غير المؤكدة، فقد تشمل قاعدة البيانات أيضًا حوالي 47.000 من الهويات المدرجة على ما يُسمِّى بـ "قوائم الممنوعين من السفر"، وكذلك حوالى 860000 من الملفات البيومترية، خلال سنوات العمليات القتالية النَّشِطة في العراق وأفغانستان كان الجيش الأميركي هو المسيطر على المعلومات البيومترية وبيانات الهوية في قاعدة البيانات TIDE ، ومع ذلك تُشير التقارير الصحفية غير المؤكَّدة أن السيطرة قد تحوَّلت في السنوات الأخيرة إلى إدارة المخابرات وإدارة تطبيق القانون الفدرالي والمحلي بشأن تقديم معلومات الهوية الجديدة وتقديم ترشيحات قائمة المراقبة.

وقد تطوَّر هيكل المعلومات المماثلة أيضًا حول جمع وتخزين بيانات الحمض النووي، وقد استُخدِمت هذه البيانات لدعم تحقيقات تطبيق القانون؛ ومع ذلك تَزايدَ تطبيقها على الأمن القومي ووزارة الدفاع، ومتطلبات الاستخبارات، قامت قوة مجلس العلوم الدفاعية 2007 بالقياسات الحيوية بوصف مفهوم

مكافحة الإرهاب من خلال الطب الشرعي في وزارة الدفاع بعد أحداث11/9 ؛ بأنه قد عمِل على تطوير "مخزن آمن وقاعدة بيانات تفاعلية، التي ستركِّز على حِفظ واسترجاع، وتفسير البيانات البيولوجية الجزيئية لتحديد وتتبُّع المشتبه في صِلتهم بالإرهاب.

وقد قام مختبر القوات المسلحة بتحديد مثل هذه" القوة" لقاعدة بيانات الحمض النووي، بما في ذلك لمحات من المعتقلين بعيدًا عن الولايات المتحدة، وجمع الحمض النووي المجهول نتيجة الغارات، والأدلة الجنائية في مواقع حساسة أخرى، وبحلول عام 2007، وَرَد أن قاعدة البيانات المشتركة الاتحادية لوكالات استخبارات الحمض النووي تتضمَّن أكثر من 15.000 عينة من الحمض النووي، مع ضعف عدد العينات التي تنتظر أن يتم معالجتُها خلال سنوات العمليات القتالية النَّشِطة في العراق وأفغانستان، وكانت وزارة الدفاع هي العميل الرئيس لهذا التحليل؛ ومع ذلك، فقد تم دعم قاعدة البيانات أيضًا من خلال مجتمع الاستخبارات، وتطبيق القانون المحلي، وتحقيقات مكتب التحقيقات الفيدرالي في جهود مكافحة العبوات الناسفة.

كما يوفِّرُ مختبرُ البحث الجنائيِّ التابع لجيش الولايات المتحدة (USACIL) بيانات الحمض النووي الذي يتم إدخالها في مؤشِّر نظام مكتب التحقيقات الفيدرالي المشترك (CODIS) DNA الذي يسمح للدولة الاتحادية، ومختبرات الجريمة المحلية، والبحث، بتبادل الحمض النووي إلكترونيًّا، اعتبارًا من أواخر عام 2014، فإنَّ قاعدة بيانات CODIS في مكتب التحقيقات الفدرالي تحتوي على ما يزيد عن 11 مليون من ملامح المذنبين، مليوني شخصية معتقلة، وما يَقرُب من 600.000 لمحة من الطب الشرعي، وعلى الصعيد الدولي، فإن نحو 30 بلدًا لديها قواعد بيانات مماثلة مثل CODIS؛ حيث تقوم باستخدام المعايير التقنية المتوافقة مما يجعل من الممكن المقارنة بين قواعد البيانات الوطنية.

كما يدعم USACIL نظام مؤشر الحمض النووي الوطني (جزء من CODIS) عن طريق توفير عينات الحمض النووي من الاهتمامات المتعلقة بمخاوف إنفاذ القانون وهُويات المحتجزين ومكافحة الإرهاب.

مع ذلك، فإن قاعدة البيانات في الغالب تُوصَف باسم "القوة الزرقاء Blue Force" للعينات المستخدَمة في المشرحة والتحقيقات الجنائية، ولا يتمُّ ملؤها بما فيه الكفاية مع تشكيلات الهدف التي تجعلها تستجيب تكتيكيًّا للاستهداف التنفيذي.

بالإضافة إلى تحسين تكامُل البيانات والأدوات التحليلية، فقد ساعدتِ التَّطوراتُ الأخيرة الأخرى في جَعْل التقنيات الحيوية والطب الشرعي قابلة للتطبيق عمليًّا على مدى العقد الماضي، بما في ذلك تقنيات التصغير وقابلية جمع الأجهزة، وقد تمَّ تطويرُ نموذج الولايات المتحدة لنظام التحقق من الهُوية الذي وُضِع أصلًا في عام 1999 من قِبل مختبر قيادة معارك الجيش أساسًا للاستخدام في المنشآت الثابتة لإدارة الوصول إلى منظمة القاعدة في منطقة البلقان. ولم تكن التكنولوجيا الأصلية متنقِّلة للغاية، وكانت تَفتقِر إلى الربط في الوقت الحقيقي إلى خدمة المناطق النائية لنقل البيانات وتحديثات قائمة المراقبة، وقد أدَّتِ المتطلبات التنفيذية التي واجهتها في العراق في وقت مبكِّر إلى المزيد من الجهود المبذولة لتحسين الاتصال عن بُعدٍ كما رأينا في التكرار اللاحق لأفضل التقنيات المتاحة وفي وقت لاحق في نظام وكالات الهوية التي تم نشرها عام 2007.

تَتَّبع علومُ الطبِّ الشرعيِّ مسارًا مماثلًا مع تَطوُّر مختبراتِ الطبِّ الشرعيِّ المتنقِّلة والمحمولة داخل الوحدات العسكرية. وقد صُمِّمت هذه "المختبرات القابلة للقياس على وجه التحديد للنقل البريِّ التكتيكيِّ ورفْع الأمور مع الفنيين لدعم تحليل الطبِّ الشرعي، عَرضتِ المختبراتُ مجموعةً كاملةً مِن قدرات الاستغلال التي كانت عادة متاحة فقط في مرافق المختبرات الثابتة قبل 11/9، وتَشمل هذه القدرات الاستطلاعية الجديدة تحليلَ البصمات الخفية، والحمضَ النوويَّ والأسلحةَ الناريةَ وعلاماتِ الأدواتِ، وتأثيرَ المواد

الكيميائية، واستغلالَ وسائل الإعلام، كما أظهرت هذه التقنيات فائدتها للكشف على أساس الهوية والاستهداف في العراق وأفغانستان، وقد بدأ الاستخدام داخل إدارة إنفاذ القانون المحلي، ودائرة الهجرة، ووظائف الرقابة الحدودية.

على سبيل المثال، فقد تمَّ تصميم نظام التحقق من الهُوية الجديد في مكتب التحقيقات الفدرالي لتعزيز الترابط، وصولًا إلى سلطات إنفاذ القانون المحلية مع الأجهزة المحمولة لجمع البصمات وردود الفعل في الوقت الحقيقي في مقابل قاعدة البيانات الجنائية في مكتب التحقيقات الفدرالي. وبالمثل، يَستخدِم نظامُ صور الطريق السريع الآن تَقنيةَ التعرف على الوجه للبحث عن الصور المشبوهة في مقابل صور ملايين الهويات الجنائية المعروفة، وتَدرُس الجماركُ الأمريكية وحماية الحدود الدروسَ المستفادة تحديدًا في العراق وأفغانستان من أجلِ تطبيق الأدوات والأساليب المماثِلة لبرامج الفَحص على أساس الهُويَّة وعملياتها في المناطق النائية على طول الحدود، وأدَّى ذلك إلى بَرْنامج التَّمكينِ مِن الجمع البيومتري للمطابقة ضد قواعد البيانات على المستوى الوطني من الهويات الإجرامية والإرهابية، بدأتِ الوكالة أيضًا في القيام ببرنامج تجريبي باستخدام التكنولوجيا الجديدة للتعرف على الوجه لمقارنة صور جوازات السفر مع وجوه المسافرين من أجل الكشف عن وثائق السفر غير الشرعية.

وباختصار، وعلى مدى العقد الماضي، أضاف تَزايدُ الحرب الإلكترونية نموذجًا تنفيذيًّا جديدًا؛ حيث يتميَّز نَهجُ الحرب الإلكترونية بثلاثة عناصر متميزة: إضفاء الطابَع الفرديِّ، والهوية، والمعلومات، وقد استَنَد هذا التحول على التصنيف المنتظِم لتهديد الأمن القومي وصولًا إلى أدنى مستوى تكتيكي والأولويات الاستراتيجية في مواجهة التهديدات الناشئة من المؤسسات غير الحكومية والمقاتلين الفرديين، وقد أدَّى هذا التركيز التنفيذيُّ إلى خَلْق فترة من الابتكار والتقنية التي تركِّز على فَحْص هُويَّة القاعدة وأشكال الاستهداف العسكريِّ الشخصي للغاية، هذا النمط الجديد من الحرب يقوم على المستوى

الأساسي لتكنولوجيا المعلومات التي سَمحتْ بجمع البيانات وتبادُلها، عَبْر جهاز الأمن القومي الأمريكي بأكمله بكفاءة غير مَسْبوقة.

وتَعكِس هذه الظواهرُ الدِّيناميَّة التنظيميَّة الأكبر، التي ترتبط ارتباطًا وثيقًا بنموذج الحرب الإلكترونية، على وجه التحديد توضِّح كيف أدَّى هذا الشكلُ مِن أشكال الحرب إلى التآكل التدريجي للحدود التقليدية التي تَفصِل العمليات العسكرية والاستخبارات الأجنبية، والمهام الأمنية المحلية، بالإضافة إلى ذلك، فقد ركَّزت استراتيجية الأمن القومي الأمريكي على التهديدات التي يُشكِّلها مقاتلون من الأفراد والجهات الفاعلة غير الحكومية، التي قامت بإعداد السياق السياسي للحرب دائمًا مع عدد قليل من الحدود الجغرافية أو الزمنية الملحوظة. يُعتَبر القسمُ التالي مِن تَزايدِ الحرب الإلكترونية في سياق هذه القرارات السياسية من الآثار المترتبة على مستقبل استراتيجية الأمن القومي.

قدَّمتِ الإتجاهاتُ الجديدةُ والتكنولوجيات الدعمَ إلى وسائل وأساليب الحرب الإلكترونية، ومع ذلك، أدَّى هذا التحولُ النوعيُّ في نهاية المطاف إلى خيارات السياسات والقرارات الاستراتيجية المقدمة كاستجابة للتصورات حول بيئة التهديدات المتغيرة، تمَّ عَملُ التفويض عام 2001 باستخدام القوة العسكرية للسياق القانوني الأوليِّ (AUMF) لشنِّ حرب ضد الشبكات والأفراد الموزعين بشكل جغرافي، وبشكل عام؛ يُجيزُ استخدامَ القوةِ ضد "الدول أو المنظمات أو الأشخاص".

وصَف مديرُ وكالة الاستخبارات المركزية المفصلية (CIA) جون برينان مؤخرًا كيف يتم تطبيق تَصوُّر AUMF الأصلي ضد مجموعة متنوِّعة من التهديدات، مشيرًا إلى أنَّه "في هذا الصراع المسلَّح، يكون الأفراد جزءًا مِن تنظيم القاعدة أو القوات المرتبِطة بأهداف عسكرية مشروعة"، ومع مرور الوقت، أصبح تطورُ استخدامِ أسلوب "القتل المستهدف" ضد أهداف قيادات تنظيم القاعدة حجرَ الزاوية في منهج الولايات المتحدة لمكافحة الإرهاب، وتمُّ استخدامه على نِطاق واسع في باكستان واليمن وليبيا وأماكن أخرى، ومع ذلك، قبل أي تقدير، تم توسيع هذا النهج بشكل أعمقَ بكثير عن الاستهداف المحدود للقيادات رفيعة المستوى، ويمثِّل الآن نمطًا جديدًا من الحرب التي تَشنُّها وسائل الهجمات الدقيقة ضد الأفراد.

يُمكن القول، بأنَّ استخدام هذا النَّهج يقوم بالتركيز الفرديِّ على مكافحة الإرهاب في مسار منطقي للديمقراطية الليبرالية للتعامل مع خَطَر الإرهاب، في الوقت الذي يسعى فيه أيضًا إلى تحقيق تَوازُن الحريات المدنيَّة في المجتمع المتعدد، عدم الارتياح العام في وصْف التقنيات المستَخدَمة بعد 11/9 يُسبِّب الضغطَ السياسيَّ الناجم عن الأساليب التي تركِّز بشكل خاص على الأشخاص، الذين يُعانون مِن

ارتباطات مشروعة بالإرهاب، بدلًا من اتخاذ إجراءات فئوية ليتمَّ تطبيقها ضد مجموعات مشبوهة بأكملها (عرقية أو إثنية أو دينية أو غير ذلك)، وفي الآونة الأخيرة، أصبح تطبيق القلق الشعبي واسع النطاق على مدى المراقبة الداخلية من خلال وكالة الأمن القومي (NSA)؛ حيث يشير إلى وجود قَلَقٍ مماثِل مع النهج الذي يُشبِه حملة التفتيش التي تشمل معظم الإشارات؛ ومع ذلك، فإنَّ الأميركيين أعربوا عن بِضعةِ تحفُّظات في جمع المعلومات الاستخبارية، والاستهداف القاتل استنادًا إلى نهجِ الأدِلَّة وقرائن الذنب، وهكذا، على سبيل السياسة، يُوفِّر شنُّ الحرب القليل من الخصوم السياسيين للإدارات المتعاقِبة.

يَبْدو أنَّ التفكيرَ المماثِلَ وراء قَبُول الجمهور العام "لقوائم المراقبة" يُقدِّم طرقًا مُصمَّمة لكشف الأفراد ذوي الصلات المعروفة أو المشتبه بهم بالإرهاب؛ فعلى سبيل المثال، يَسمَح الأمنُ القومي للتوجيه الرئاسي 2008 بجمع ومشاركة المعلومات بشأن الأشخاص الذين يُشكِّلون تهديداتٍ مُحتمَلة للأمن القومي من خلال المعلومات البيومترية، وتوجيه القليل نسبيًّا مِن اهتمام الرأي العام، دينيس سي. بلير، مدير الاستخبارات الوطنية ربما كان أفضلَ مَنِ امتَلَك أسلوبًا جديدًا ومختلفًا لتقييم المخاطر الشخصية، عندما لاحَظ أنَّ خطر الإرهاب قد يُغيِّر نهج التحذير الاستراتيجي، مشيرًا إلى أنَّ هناك الآن أسماء ووجوه يجب أنْ تَقتِرن مع التَّحذير منها، وبصفة عامة، فإنَّ الأميركيين يُظهرون بعض التحفظ تُجاه هذا الأسلوب لمكافحة الإرهاب على أساس الهوية؛ ما دام يبدو موجَّهًا إلى التهديدات المحتملة، ويتم تطبيقه بشكل عشوائي.

ولعل هذه المفارقاتِ جعلتِ الرأيَ العامَّ الأجنبي والضغط الدبلوماسي يلعبون أيضًا دورًا في دفع الولايات المتحدة نحو أسلوب الحرب الإلكترونية، والاحتياج إلى مزيد من التمييز والتخصيص لجهود مكافحة الإرهاب؛ من ضِمن الأمثلة الجديرة بالذِّكر الإدانةُ الدولية الموسَّعة الموجَّهة ضدَّ أنماط السلوك العدائي، وليس ضد أفراد معينين، هذا النهج يُشبِه أساليبَ الاستهداف التقليدية المطبَّقة ضد التشكيلات والمعدات؛ حيث تُوفِّر التوقيعات التقنية لتصنيف موثوق عمومًا للأهداف المقصودة، ومع ذلك، فقد

أدَّى استخدامُ هذه التقنية ضد الأهداف غير النظامية أو الأفراد إلى العديد من الحوادث بشكل خاطئ وسقوط ضحايا من المدنيين غير مقصودين، بما في ذلك مقتل المواطنين الأمريكان والرهائن، حتى في ظل أفضل الظروف.

وهذا النمط من الاستهداف يمكن أن يكون تحدِّيًا بطبيعته؛ كما أشار أحدُ المسؤولين في قيادة العمليات الخاصة في الآونة الأخيرة، وقال: "عندما نحاول معرفة هُويَّة الفرد بشكلٍ شخصيٍّ، فلا يوجد أدنى هامش للخطأ"، عندما تَحدُث هذه الأخطاء، فإنها غالبًا ما تُسبِّب تداعيات سياسية كبيرة، مثلما شَهِدت الولايات المتحدة في باكستان واليمن، فضلًا عن العديد من الحوادث خلال العمليات العسكرية في العراق وأفغانستان.

ونتيجة للاستجابة لهذه الضغوط، تحرَّكت إدارة باراك أوباما نحو زيادة استخدام الضربات "الشخصية" الموجَّهة ضد الأفراد المحدَّدِين؛ للتأكيد على تجنُّب ردِّ الفعل السلبي الناجم عن الخسائر غير المقصودة، هذه العملية تُفيد بأن التقارير تتم رسميًّا من خلال إنشاء مصفوفة التصرف التفاعليِّ والفردي، واستهداف قاعدة البيانات على أساس السير الذاتية، والمواقع، والروابط، والملامح الفعلية للأهداف ذات القيمة العالية؛ ومع ذلك، تُشير بعض الانتقادات إلى أنَّ هذه الضربات لم تكن دقيقة بما فيه الكفاية في تحديد الأشخاص المستهدفين، لا سيما في بعض المناطق مثل باكستان واليمن؛ حيث إن الولايات المتحدة ليس لديها قوات كبيرة أو قدرات استخباراتية على الأرض، وأشار أحدُ الخبراء في حرب الطائرات بدون طيَّار أن مُعدَّل الخسائر غير المقصودة التي لَحِقتْ به خلال هذه الضربات قد سلَّطت الضوء على حقيقة أنه حتى الوقت الحالي فإنَّ "معظم الأفراد الذين قُتلوا لم يكونوا ضِمن قائمة القتل، والحكومة لا تعرف أسماءَهم على وجه التحديد".

وكمِثال للردِّ بشكل جزئيٍّ على هذه الانتقادات، اقترحتِ الإدارة تفضيلَ سياسة الاعتقال ومحاكمةَ المشتبه بتورطهم في الإرهاب الفردي، عندما يكون ذلك ممكنًا، في ضوء المخاوف المستمرة بشأن الاحتجاز طويل الأجل من قِبل القوّات غير النظامية، فهذا الجانب من جوانب الحرب السياسية يُسلِّط الضوءَ على التوترات المتأصِّلة بين الأنشطة القتالية التقليدية ومهام إنفاذ القانون، وفي السنوات الأخيرة، فقد حان وقت الاستهداف على أساس الهُوية التي تُشبِه مذكرات الاعتقال لأكثر من حِقبة الحرب الباردة التي تستهدف الملفات، لا سيما خلال مراحل لاحقة من العمليات في العراق وأفغانستان، وارتفاع قيمة الاستهداف التي تطوَّرت نحو النهج "القائم على الأدلَّة"، الذي يَعتمد على التحقق من الهُوية وعلوم الطب الشرعيِّ لدعم الأدلة المحتملة وغيرها من المعلومات الاستخبارية، ولاحَظ أحد المراقبين كيف يُمكِن لعملية F3EAD أنْ تتطوَّر تدريجيًّا إلى التحقيق والاعتقال، ووضْعِ المحكوم عليه ضِمن الاستهداف غير القاتل.

ولا سيَّما أثناءَ تَطبيقِ استراتيجيات مكافحة التمرد، لاحَظ المراقِبون كيف بدأ الجنود في الدوريات التعامل تقريبًا مثل رجال شرطة المدنية، مع عملِ المسح البيومتري والانتقال إلى الأدلة مع كلِّ مُعتقَل، ويبدو أن هذه الأمثلةَ تَدعم التخمينات من قِبل الباحث في جامعة هارفارد؛ غابرييلا بلوم؛ حيث إنَّ إضفاءَ الطابَع الفرديِّ على الحرب قد تحوَّل تمامًا إلى طبيعة الصراع المسلَّح، وتحوَّل أكثر نحو نموذج الشرطة مع زيادة التركيز على الأضرار الفردية، الضحايا الفردية، والمسؤولية الفردية.

أمَّا السياسة العامة، فقد خَلَق نموذجُ الحرب الإلكترونية أيضًا المزيدَ مِن تحديات التقييم الاستراتيجي والإجراءات المفيدة للفعالية، خلال تاريخ الحروب الحديثة، تم تطبيق مجموعة من الإجراءات كعوامل لتقييم المناهج المختلفة التنفيذية والنظريات القتالية، والقرارات الاستراتيجية، عَرضتِ الحرب العالمية الثانية نموذجًا كميًّا بسيطًا نسبيًّا، بدعم من إمدادات لا نهاية لها من الإحصاءات عن أعداد القنابل التي أُلقيت والقوافل العسكرية والمصانع التي تمَّ تدميرُها، والأراضي التي تمَّت مصادرتها، اعتقال الجنود، وانهزام

الوحدات في ساحة المعركة. وتتناسب هذه الإجراءات أيضًا مع صراعات العصر الصناعي؛ حيث إن التحديات الاستراتيجية المركزية في كثير من الأحيان تُناسِب القضايا المعنيَّة من حيث الوقت والمسافة، وقد يتمُّ اختزال جميع المشاكل عمومًا للتحليل المنظَّم والتقييم الكميِّ، على العكس من ذلك، أنتجت فيتنام تغييرًا لهذه الإجراءات، وخصوصًا ظهور العدو كمقياس بديل لنجاح العملية في غياب نهاية الدولة السياسية العسكرية الواضحة.

تمَّ استبدالُ نموذج الحرب الإلكترونية في فيتنام مع نسخة مُعدَّلة من الإجراءات القائمة على تحليل الأثر النسبي. وحصل هذا النهج على مختلف العوامل مِثل شخصية المقاتل الفرديِّ التنفيذيِّ، والمهارات التقنية الفريدة، الشبكة المركزية، والتأثير الجهات الفاعلة داخل الشبكة التنظيمية الكبيرة، هذه التقنيات لها أسسٌ نظرية عميقة في نظرية التحليل الاجتماعي للشبكة، ومع ذلك، فإنها لا تزال تعتمِد على الإجراءات الذاتية المكثَّفة، التي يَصعُب تطبيقُها كأسلوب تقييم في الحملات العسكرية، على سبيل المثال، كانت إحدى الظواهر السيئة التي ظهرت في حرب العراق في وقت مُبكِّر هي "بطاقات تحديد الهوية"، التي صَدرتْ للقوات الأميركية؛ لتحديد هُوية الأعضاء رفيعي المستوى في حكومة صدام حسين وكبار أعضاء حزب البعث.

ثم تطوَّرت هذه البطاقات سريعًا إلى ما يُشبِه مِقياسًا غير رسميٍّ للتقدم الفِعلي على أرض المعركة؛ حيث قُتِل القادة الرئيسون أو أُسِروا، واستمرَّ تركيزُ الاهتمام على هذه الإجراءات، حتى أصبح من الواضح تمامًا أن لم يكن لديهم أهمية خاصة بالنسبة لتطوُّر فعاليات الأمن على أرض الواقع، مع مرور الوقت، تَطوَّرت أساليبُ مماثلةٌ لقياس آثار ضربات مكافحة الإرهاب ضد الشبكات المعادية، وتطبيق التقييمات النوعية لقياس الأثر العملي للقتل أو الأسر المعين "الأفراد ذوي الأهمية العالية"، ومع ذلك، كما هو الحال مع أعداد القتلى في فيتنام، هناك خدعة كامنة في هذا الأسلوب، فبغضِّ النظر عن عدد مرات اغتيال "حركة

الشباب الثاني"، قد يكون هناك دائمًا "حركة شباب ثاني" أخرى؛ لكِنْ في المقابل، سَقطتْ برلين مرة واحدة فقط.

مسألة التقييم التنفيذي تُثير قضية أكبرَ مِن حيث تقييم نموذج الحرب الإلكترونية على حدٍّ سواء، باعتبارها خيارًا سياسيًّا وكعنصر من عناصر الاستراتيجية العسكرية، في حين أن هناك القليل من الجدل فيما يتعلَّق بالكفاءة التكتيكية المذهلة لتقنيات الولايات المتحدة لتحديد واستهداف المقاتلين الفرديين في ساحة المعركة، فما هو أقل تأكيدًا ما إذا كانت هذه الأساليب تتجمَّع في استراتيجيات فعَّالة لتحقيق أهداف سياسية أكبر، يقدم التجديد الدائم للتهديدات الإرهابية داخل باكستان واليمن والصومال أدلةً كافيةً على أن الاستهداف على أساس الهُوية كان ناجحًا تمامًا باعتباره حجرَ الزاوية في استراتيجية مكافحة الإرهاب.

وبالمثل، فإنَّ الأوضاع المتدهورة في العراق وأفغانستان تُشير إلى حدود هذه الأساليب التي يمكن أن تتحقَّق باعتبارها عنصرًا رئيسًا من مكافحة التمرد، على العكس من ذلك، يمكن للمرء أن يُقدِّم المطالبة القوية التي أسهمتْ بمزيج من هذه التقنيات، جزئيًّا أو كليًّا، لحماية الوطن بنجاح من أي هجوم إرهابي كبير منذ 11/9 من خلال تحديد التهديدات الفردية وتعطيل شبكاتهم، ويثير الغموض الكامن في البيانات؛ المسألة الأكثر صعوبة عمَّا إذا كان يمكن للمرء أن يُقيِّم بفاعلية فائدة التكتيكات والأدوات المحددة بشكل مُنفصِل عن نتائج الاستراتيجية الشاملة التي تُنتِجها، كما حذَّر ماكماستر، مدير مركز التكامل والقدرات التابع للجيش مؤخرًا، من "الاستهداف المتساوي غير الاستراتيجي".

وقد أشار الرئيس أوباما خلال الخطاب الأخير لجامعة الدفاع الوطني أنه "يجب أن نُحدِّد طبيعةَ ونِطاق هذا الصراع، وإلَّا فإنه سوف يعمل على تحديدنا وتقييدنا"، وبالفعل، كان هذا إلى حدٍّ كبير هو الحال بالنسبة لمؤسسة الأمن القومي الأمريكي منذ 9 / 11، وعلى مدى السنوات الـ 15 الماضية، خَضعتْ هذه الأساليب التقليدية إلى ثورة في الشكل والمضمون، وتوجَّهت نحو التركيز باتجاه نموذج الحرب

الإلكترونية المختلف كثيرًا عما كان في عهد الحرب الباردة، وقد وضَعتْ هذه الكِيانات منهجياتٍ جديدةٍ وتقنيات وأساليب تحليلية تَعكِس إعادة توجيه أولويات الأمن القومي على أساس مُهمَّة هزيمة شبكات الخصوم واستهداف المقاتلين الفرديين، كما لاحظ ضابط أمريكي كبير في الآونة الأخيرة، أنَّ مهمة "وضع قيادات العدو على رأس الأولويات" أصبحت وظيفة عسكرية أساسية، ويمكن القول: إنَّ انعكاس النموذج الجديد للأمن الوطني يركِّز على هزيمة التهديدات من الجهات الفاعلة غير الحكومية، شبكات الخصوم، والمقاتلين الفرديين.

ووَفْقًا لجميع المؤشرات، فإنَّ بعض أشكال الحرب الإلكترونية/ الذكية ستبقى مستمرة كنموذج لأمن الدولة ومنهجية الحروب الأميركية في المستقبل، وتتَّسِم التحديات الأمنية المعاصرة بضرورة إجراء العمليات العسكرية المناطق ذات الحوكمة السيئة، التي تُعاني من أنظمة ضعيفة فيما يتعلَّق بتحديد هُويَّة الأفراد، وضد الخصوم العازمة على استخدام مَيزةِ عدم الكشف عن هُويَّتها لمصلحة فعليَّة، وفي الوقت نفسه، فإنَّ تهديدات الإرهابيين متعدِّدي الجنسيات تظهر مؤشرات محدودة تدلُّ على احتمالية تقلُّصها، لهذه الأسباب السابقة فإنَّ الأهمية العملية لاستراتيجيات تحديد الهُوية في ساحات المعارك الحديثة وعلى طول الحدود، تَزداد من حيث الأهمية.

الحرب الإلكترونية كدراسة حالة للابتكار العسكريّ

يُعدُّ تزايدُ الحرب الإلكترونية بمثابة دراسة حالة لعناصر الابتكار العسكري، فقد تطوَّر نموذجُ الحرب نتيجة تحدٍّ أمني وطني صارم للغاية، بعد أحداث الحادي عشر من سبتمبر 11/9، ويركز هذا الابتكار التقني على الحاجة الملحَّة للتحديد والفحص، واستهداف المقاتلين الفرديين كجزء من الشبكات الموزَّعة. في البداية، مثَّلت هذه المهمة تحدِّيًا تنفيذيًّا؛ حيث كان جهاز الأمن القومي الأمريكي غيرَ مُستعدٍّ إلى حدٍّ كبيرٍ؛ فلم تكن قبل 11/9 الإجراءات الروتينية والاستراتيجيات القتالية هي الخيار الأمثل للعمل عبر ساحة المعارك اللامحدودة، وضد تهديدات التكتيكات التي لم تتَّفق مع الاختلاف الواضح بين العمليات العسكرية الأجنبية والمهام الأمنية ذات المستوى المحلي، وفي هذا المعنى، فإن تَزايدَ الحرب الإلكترونية يكون بمنزلة مِثالٍ مُفيدٍ لدراسة الابتكار في زمن الحرب.

ينظر علماء الابتكار العسكري عمومًا إلى عدَّة عوامل للحصول على الأدلة من خلال التغييرات الجوهرية التي تطرأ. العامل الأول: هو أن عملية الابتكار تغيِّر الطريقةَ التي تَعمَل بها التشكيلاتِ العسكرية في هذا المجال، والثاني هو أن هذه التغييرات مهمَّة مِن حيث النِّطاق والتأثير التنظيمي، والثالث هو أنَّ هذه التغييرات تنتج في نهاية المطاف زيادة الفعالية العسكرية، من خلال هذا المعيار، فإنَّ تَزايدَ الحرب قد استوفت إلى حد كبير العنصرين الأوَّلَيْن، ومع ذلك، لا يزال الثالث قابلًا للنقاش، وهذا يتوقَّف على نطاق التحليل وشروط الإجراء.

هناك سؤالٌ منفصلٌ ولكنه يتعلَّق بهذا الموضوع، وهو ما إذا كانت الحرب الإلكترونية تمثل حقًّا نموذجًا تنفيذيًّا جديدًا أو مجرَّد تَكرار للأفكار والأساليب القديمة، ولكن يتمُّ تنفيذُها بتكنولوجيات حديثة، ويمكن القول: إن المرء يمكنه تحديدَ العناصر التي تمهِّد للحرب الذكية/ الإلكترونية، مثل ما حدَث خلال

برنامج فينيكس الخاصِّ بوكالة الاستخبارات المركزية في فيتنام، وفي الآونة الأخيرة، ما حدث مع أساليب الاستهداف الإسرائيلية المستخدمة في غزة ولبنان، كما هو الحال مع الحرب الإلكترونية، حيث تُشارِك هذه الأمثلة أيضًا في النَّهج التنفيذي على أساس تحليل الشبكات المركزية وأساليب الاستهداف الفردية.

ومع ذلك، فقد قدَّمتْ عِدَّة جوانب هامة يمكن القول: إنها تجرِبة فريدة أصبحت حديث الولايات المتحدة في تلك الفترة، وكان من أبرز هذه الاختلافات هو نطاق التطبيق، وقد اتخذت عمليات نموذج الحرب على نطاق عالمي مَكَّنَ مِن تحوُّل الأساليب التقليدية الهائلة إلى أساليب العمليات العسكرية المتكاملة، والتكامل مع أنشطة المخابرات الأجنبية، والمهام الأمنية الداخلية على مستوى التاريخ الأميركي. وتقوم هذه الاستراتيجية على مجموعة مُتنوِّعة من الابتكارات التقنية الجديدة غير المعروفة عَمليًّا على أرض المعركة قبل 11/9، بما في ذلك الطائرات بدون طيار، والقياسات الحيوية، والطب الشرعي الاستطلاعي، وتحليل الحمض النووي، وأدوات إدارة المعلومات المتقدمة، وذلك على سبيل المثال لا الحَصر.

حيث إن تطبيق هذه الأدوات يعكس التحول نحو وجهة النظر بأنّ تمحورَ المعلومات العسكرية يختلف تمامًا عن النموذج التقليدي في حِقبة الحرب الباردة، وقد شَمِل هذا التحولُ والتطورُ في النظرية القتالية التي أدخلت أساليب جديدة في الإتجاه التطوري مِثل تحليل الشبكات الاجتماعية وأساليب الاستهداف القائم على الهُوية، وقد تركَّزت كلُّ هذه التغييرات على الأساليب الاستراتيجية المتَّبعة، وأحدثتْ تغييرًا جوهريًّا؛ حيث إنَّ أولويات المؤسسات غير الحكومية والمقاتلين الأفراد أصبحت على قَدمِ المساواة مع التهديدات التي تُشكِّلها الجهات الحكومية في تشكيل سياسة الأمن القومي.

تمثِّل هذه التغييرات أيضًا تحولًا خفيًّا، ولكنه عميقٌ في التفكير بشأن كيفية تطبيق الأساليب العسكرية ضد هذه التهديدات، وبذلك يتم إعادةُ تعريف دور الهُوية في الحروب الحديثة، في تحليل هذه التغيرات، يقترح بعض العلماء أن عملية الابتكار في زمن الحرب يَنْبغي النظر إليها كظاهرة متميِّزة عن التغيير

والابتكار في وقت السِّلم، يمكن القول: إن تلك الطرق العرضية المتعلقة بابتكارات الحروب تميل إلى حد ما لتكون أقل تعقيدًا، كما أنها تستجيب للغاية للظروف الطارئة، ويرجع هذا جزئيًّا إلى حقيقة أن الصراع النشط يُقدِّم مُختبرًا لـ "التجارب الطبيعية"، حيث يُعبِّر عن المتطلبات القتالية بشكل واضح في الاستجابة إلى تصرفات العدو فورًا بدلًا مِنَ افتِراضها.

يوفِّر هذا الوضعُ اختبارًا صعبًا لردود الفعل التكتيكية المباشرة، وبالتالي خَلَقَ فعالية قوية لتصميمات تكرارية محددة "نمط معين متبع"، والعمل على تحسين إجراءات الاستجابة السريعة، هذه العوامل لها تأثير على كيفية قيام الاحتياجات التنفيذية بتحديد وتسريع الإجراءات المتَّبَعة من البحث والتطوير، والنماذج، والتوظيف، ومع ذلك، فإنَّ التغيير المؤسسي السريع لا يزال يتطلَّب حافزًا فكريًّا أوليًّا ليكون بمثابة دافع منهجيٍّ لتحديد استراتيجية الابتكار، بدون الفكرة المتماسكة التي توفِّر الإطارَ الفكريَّ العامَّ، فإنَّ مجموع مُخرَجات الابتكار سيكون حتمًا أقلَّ مِن أجزائه المنفردة.

في حالة الحرب الإلكترونية، كانت هذه الفكرة المركزية تمثِّل إثباتًا بأن القتال ضد الشبكات والأفراد بحاجة إلى منهجيات مختلفة تمامًا ومجموعة أدوات بخلاف الأساليب القياسية المتَّبَعة في الصراعات التقليدية، بمجرَّد أن يتمَّ تأسيس هذا الإطار المنهجيِّ الشامل، فإنَّ عملية الابتكار العسكري تحدَّث بسرعة في مجالات متعددة، المجال الأول تضمَّن تغييرات النظرية القتالية التي تُرجِمت إلى تصميم تطوريٍّ ومستوى أعلى من مفاهيم العملية، يتضمَّن المجال الثاني اعتمادَ أدوات وأساليب فنيَّة مُتخصِّصة يتمُّ تطبيقُها مباشرة على المشاكل التكتيكية لخَلْق تأثيرات في ساحة المعركة. وكان المجال الثالث هو عملية أبطأ مِن تغيير السلوكيات التنظيمية والقيم المؤسسية، والأفكار الفلسفية حول كيفية تصوُّر الخدمة العسكرية لدورها وتحديد المهام داخل المؤسسة الأمنية الوطنية الكبيرة.

في هذه المرحلة، يتمُّ وصْف الحرب الإلكترونية في النموذج التنفيذي بأنها تقع على مفترَق طُرق، ويُعتبر التحدي المقبل هو تحديد عوامل النموذج/ المنهجية التي ستظلُّ وثيقة الصِّلة بمواجهة التحديات الأمنية المستقبلية وأولويات الدفاع الأمريكية العامة، وهذا يتطلَّب تقييمَ الدروس المستفادة من العقد الماضي، وتطوير النظريات والتقنيات الداعمة، وتحديد الأولويات للتدريب، ومن ثم بناء الأسس المؤسسية لدعم القدرات المطلوبة، أن واحدة من أَصعبِ جوانبِ هذه المهمة هي اختيار التقنيات الصحيحة في غياب التحدي التنفيذي المستمر للعدو المحدَّد بوضوح.

حتميًّا، أن ديناميات وضرورات الابتكار التي تُتَّخذ "وقت السلم" سابقًا، سوف تختلف عن الابتكار في زمن الحرب. ومن المرجَّح أن يزداد تأثيرُها وتقومَ بتشكيل الجدل حول النظرية القتالية والتطوير المنهجيِّ، واستراتيجيات الشراء، والأدوار المؤسسية وبالتالي الأولويات الأخرى، في حالة الحرب، سوف تحتاج الولايات المتحدة إلى الاحتفاظ ببعض الأدوات والأساليب المتخصِّصة لغرض تمييز الصديق من العدوِّ ومكافحة الخُصوم والشبكات، ولا توجد أي إشارة بأنَّ التهديدات الصادرة عن الجهات الفاعلة غير الحكومية سوف تتناقص قريبًا، وأنه لن يكون هناك تهديدٌ "الصراعات المختلطة"؛ حيث مُحارَبة المقاتلين الفرديين غير المميزين بزيٍّ موحَّد وغيرهم من التشكيلات التقليدية.

ومن المرجَّح أن تقوم الولايات المتحدة بعمليات داخل المناطق التي تتَّسِم بأنظمة ضعيفة على مستوى تحديد الهُوية أو في حال غياب هذه الأنظمة تمامًا، وكثير من هذه التحديات تُواصِل المطالبة بمكان لأدوات وأساليب الحرب، مع أخذ هذا الواقع في الاعتبار، يتناول القسمُ التالي تصوُّرَ عن التكنولوجيا الناشئة ويحاول تحديدَ بعض التوجهات العامة، التي من المحتمل أنْ تُشكِّل كيفية شَنِّ الحروب على مستوى الأجيال القادمة، وقد أظهرتِ العديدُ من هذه الأدوات بالفعل فعاليتها على أرض المعركة وتأمين الحدود، بما في ذلك القياسات الحيوية، والطب الشرعي، والتكنولوجيا، وإدارة المعلومات، وتحليل البيانات.

وسوف تستمرُّ هذه المجالات في التطور، ومن المرجَّح أن تتعزَّز من خلال الابتكارات في مجالات أخرى، بما في ذلك الأساليب البيومترية الجديدة، وتحسين أدوات الطب الشرعي الخاص بالحمض النووي، والأدوات الإلكترونية واستغلال وسائل الإعلام الاجتماعية، وتحليلات البيانات، والتعلم الآلي، والتحليل الحسابي، وغيرها.

هذه المهمة الخاصة بالتنبُّؤ بمستقبل التكنولوجيا تعتبر محفوفة بالمخاطر، إن تقديرات ما قد ينشأ من أدوات، وكيف سيتم استخدامها، والآثار المترتبة على استخدامها يظهر حتما قدرًا من السذاجة الظاهرية، ومع ذلك، هذه التكهنات تمثِّل خطرًا حقيقيًّا يُواجه المخططين والمفكرين الاستراتيجيين، حيث يجِب تخصيصُ مواردها اليوم استنادًا إلى التوقعات المسبَّبة لِما قد يحدث غدًا؛ لهذا السبب، فإن الجزء التالي من هذه الدراسة يُقدِّم عدة مجالات للتكنولوجيا الناشئة من خلال سيناريوهات الحرب الافتراضية التي تضمُّ المقاتلين الأجانب المشتبه بهم، في حين أن التفاصيل والأحداث تُعدُّ مُتخيَّلة، إلا أنها تمثِّل معضلةً أمنيةً حقيقية مصغَّرة بالنسبة للحروب وتتناول التحدي المستمر من تحديد وفحص واستهداف الخصوم الفرديين المصممين على استخدام عدم الكشف عن الهوية للمصلحة الفعلية (انظر الرسم البياني 1).

	الحرب في الحقبة الصناعية	**الحرب الإلكترونية**
السياق السياسي	مُعاهَدة وستفاليا: يتم اعتبار الجيوش المحترفة وكلاء سياسيين لتحقيق أهداف جغرافية سياسية محددة. وتسري عليهم مختلف قوانين وتشريعات الحروب.	ما بعد مرحلة معاهدة وستفاليا: مقاتلون فرديون يقاتلون لأسباب أيديولوجية وأهداف غير مُعلَنة. تتحدَّى القوانين والتشريعات التقليدية للحروب.
خصائص الخصم	جيوش الدولة: تتألَّف من الجنود المحترفين "عامة" باستخدام تشكيلات تنظيمية منهجية، وأداء غير شخصيٍّ، وأسلوب تقليدي البيروقراطي.	كِيانات من غير الدول ومقاتلين "غير مميزين" باستخدام عدم الكشف عن الهُوية من أجل بعض المزايا التنفيذية؛ استخدام تكتيكات ذات طابَع تتَّسِم

		بالخصوصية، التي نظَّمتها شبكات شخصية للغاية.
البيئة التنفيذية	تَحدُث النِّزاعات بشكل أساسيٍّ في النطاقات الطبيعية (البرية والبحرية والجوية) وتخوضها في ساحة المعركة الخطية المتجاورة. تحدُّدها حدودٌ عملية واضحة.	تَحدُث النزاعاتُ بشكلٍ أساسيٍّ في المجالات المعلوماتية (القدرة على التأثير، وعوامل تحديد الهوية، والخصائص البشرية)؛ وتكون مكانيًّا وزمانيًّا غير محدودة. يتم التعرفُ عليها من قَبْل دمج المجالات الأمنية الخارجية والداخلية للدراسة.
نظريات خوض الحروب	تخضع لأساليب المناورات العسكرية: تتَّسِم بالشدة، قوة النيران، وتدمير قوات العدو، والاستيلاء على الأراضي الرئيسة، والتركيز على المستوى العملي للحرب.	تخضع لمكافحة التمرد ومكافحة الإرهاب: تتَّسِم الإجراءات السكانية التي تركِّز على وسائل مِثل إنفاذ القانون، دمْج المستويات التكتيكية والاستراتيجية للحرب.
المنهج التحليلي والأدوات	أمر تحليل المعركة والمؤشرات والتحذيرات (I & W) من خلال الطرق والنظام الأساسي المركزي النموذجي التطوري، النماذج التحليلية التقليدية، والخصائص التقنية والاستخبارات والمراقبة والاستطلاع (ISR).	التحليل الاجتماعي للشبكة، الهجوم على الشبكات، الاستخبارات القائمة على الهوية (I2)، ونموذج إنفاذ القانون التحليلي، والخصائص البيولوجية والطب الشرعي وتوثيق واستغلال وسائل الإعلام.
نموذج الاستهداف	استهداف الوحدات العسكرية، التشكيلات والمعدات القائمة على الوضع المحدد جيدًا، وقواعد الاشتباك المتَّبَعة.	الاستهداف ضد الأفراد والخلايا، والشبكات القائمة على الهوية، الاشتباك الغامض القائم على الأدلة.
أهداف ومقاييس الفاعلية (MOE)	الاستنزاف والتدمير المادي لقدرات القتال الحربي لدى الخصم، التقييم الكمي – الوحدات المدمِّرة والاستيلاء على	استنزاف القيادات الرئيسة، والمتخصِّصين وتقييم عمليات الاغتيال النوعي / القبض على الأفراد مثيري الارتياب،

	الأراضي، يتم MOE استنادًا إلى تقييم أضرار المعركة التقنية.	يكون MOE مرتكِز على نظريات SNA للشبكة المركزية والقدرة على التأثير والتماسك التنظيمي.
معايير النجاح والوضع النهائي	التركيز بشكل أساسي على هزيمة القوات العسكرية المعادية، الاستسلام السياسي، وإطلاق الصراح المنظَّم وإعادة المقاتلين المحتجزين.	التركيز بشكل أساسي على تخفيف المخاطر بدلًا من الانتصار العسكري، عدم التسوية السياسية، الإهمال القانوني للمقاتلين المعتقلين، ومشاكل العودة إلى الإجرام الدائمة.

الشكل 1 – الحروب في الحقبة الصناعية في مقابل الحرب الإلكترونية



مستقبل الحرب الإلكترونية

تَعكِس العديد من المحفِّزات التي دفعتْ إلى ظهور نموذج الحرب الإلكترونية الكثير من التوجهات الجارية التي لا يحتمل أن تتراجع في المستقبل القريب، ومن منظور السياسة، فهناك سبب لتوقع بعض الاستمرار للمنهجيات القائمة على الرصد المستمر للتهديدات الفردية، والفحص على أساس الهُوِيَّة، والاستهداف القائم على العوامل الشخصية، إن استخدام مثل هذه الأساليب لا يزال مثيرًا للجدل نسبيًّا من المنظور السياسي، والرئيس أوباما قد أوضح رؤيته لاستراتيجية مكافحة الإرهاب التي صُمِّمت لتكون "استجابة دقيقة لمشكلة محددة جدًّا"، أمَّا التوجه المهمُّ الآخر الذي من المرجَّح أن يظلّ ثابتًا هو عدم الكشف عن الهُوِية باعتباره محفزًا تنفيذيًّا للعديد من خصوم الولايات المتحدة.

وقد أبرزت الصراعات الأخيرة في سوريا، أوكرانيا، وغيرها بوضوح هذه الحقيقةَ، وأشار معلِّق واحد مؤخرًا، في الحروب الحديثة: "إن معرفة اسم الشخص على الجانب الآخر من ساحة المعركة تتمُّ باعتبارها ضرورة استراتيجية في الوقت الحالي".

ويتناول القسم التالي مزيدًا من التفصيل حول العديد من العوامل التي من المرجح أن تعزز الدعائم الأساسية لنموذج الحرب الإلكترونية. وتشمل هذه الخصائص بيئة التهديدات، اتجاهات التكنولوجيا الناشئة، والمعنى المتغير لمصطلح "الهوية".

يبدو أن العديد من الإتجاهات المستمرة في بيئة التهديدات المعاصرة مِن المرجَّح أن تقوم بتضخيم العديد من المحفِّزات الأصلية التي أدَّت إلى نموذج الحرب الإلكترونية مؤخرًا، وصَف الأمين العام "ماك ماستر" الانتقال من نموذج الحرب الباردة، حيث كانت الدول هي المصدر الرئيس للتهديدات، على النقيض من التهديدات اليوم: تظهر الأطراف الفاعلة غير حكومية والتقاء شبكات المتمردين والمنظمات الإرهابية أكثر في شبكات الجريمة المنظمة العابرة للحدود، والحصول على القدرات التي لم يكن لديهم في الماضي.

وتشمل هذه التهديدات زيادة احتمالات نشوب الصراعات المختلطة؛ فقد لا تَنطبِق أساليب الاستهداف القائمة على الحالة التقليدية بسهولة، فضلًا عن مجموعة واسعة من الخصوم العازمة على الاستفادة من الميزة التنفيذية.

وصَف تقريرُ الإتجاهات العالمية لمجلس الاستخبارات الوطنية مؤخرًا البيئةَ الأمنيةَ شِبه المستقبلية التي تُهيمِن عليها أشكال مختلفة من عدم انتظام حرب الإرهاب والتخريب والتمرد، والأنشطة الإجرامية، أشارت شهادة من مدير المركز الوطني لمكافحة الإرهاب أن هذه الشبكات قد نمتْ في الواقع بشكل أكثر خطورة مع مرور الوقت بسبب تآكل الحكم الرئيس، مما جعلها "أكثر انتشارًا جغرافيًّا؛ حيثُ تَنْطوي على تنوُّع أكبر من الأطراف الفاعلة" وقادرة على التكيف على نحو متزايد وتهديد معقد، روبرت كارديللو، رئيس وكالة الاستخبارات الوطنية الجغرافية، لاحظ في الآونة الأخيرة أن هذه الجماعات والأفراد تعمل "حرفيًّا دون حدود جغرافية"، وبالتالي تكون أقلَّ عُرضة للأساليب العسكرية التي تستهدف الأسلوب التقليدي.

كان هناك أيضًا تحولٌ واضحٌ في تكتيكات الإرهاب بعيدًا عن العمليات النادرة، ولكن بشكل مذهل نحو نمطٍ من أصغر الهجمات، وظهر أكثر في الأفراد اصحاب التطرف الذاتي والمجموعات الصغيرة التي تعمل بشكل مستقل عن الإتجاه المركزي، اقتَرح التقرير الإتجاهات العالمية التالية:

إنَّ الأفراد والمجموعات الصغيرة لديها قدرٌ أكبرُ مِن الوصول إلى التكنولوجيات القاتلة والمدمِّرة لتمكينهم مِن ارتكاب العنف على نِطاق واسع القدرة الذي كان سابقًا حِكرًا على الدول.

ومن المتوقع أن تعزّز الجوانب الرئيسة للحرب الإلكترونية، ولا سيما اعتماد الولايات المتحدة على الجمع الفني، والفحص على أساس الهوية، واستهداف تركيز الجهود ضد الجهات الفردية، والخلايا الصغيرة، وشبكات التحدي المتمثِّلة في الدفاع ضد مثل هذه التهديدات المتنوِّعة، ويتضمَّن التحدي المباشر الناشئ عن قضية المقاتلين الأجانب.

الوضع السوري الحالي هو مثال على الحجم الهائل لمشكلة المقاتلين الأجانب، والذى يتفاقم نسبيًّا من خلال التنقل عبر الحدود والتجنيد وعدوانية وسائل الإعلام الاجتماعية، ووَفْقًا للتقديرات الأخيرة، فقد انضمَّ ما يصل إلى 20.000 مقاتل أجنبي من نحو 90 دولة من مختلف الفصائل للقتال في سوريا، بما في ذلك الآلاف من حاملي جوازات السفر الأوروبية وعدة مئات من الولايات المتحدة، وصَف رئيس المركز الوطني لمكافحة الإرهاب مؤخرًا تدفُّقَ المقاتلين الأجانب إلى سوريا "بأنه غير مسبوق" وبمعدَّل يتجاوز بكثير حركة سفر الأجانب إلى أفغانستان وباكستان والعراق واليمن والصومال أو في أي نقطة على مدى السنوات العشرون الماضية.

خارجِ الولايات المتحدة، وضعتْ مُعظم البِلدان الاستراتيجيات الجزئية لمراقبة وتتبُّع تدفُّق المقاتلين الأجانب وصولًا إلى مستوى المقاتل الفرديِّ، على سبيل المثال، الاتحاد الأوروبي (EU) ليس لديه هناك عملية منهجية للتحقق من هُوية جميع المواطنين لإعادة دخول المنطقة من الخارج. خلال 2013 نفت تركيا دخول حوالى 4،000 شخص مُدرَج في قاعدة بيانات عدم الدخول واعتقال 92،000 شخص آخَر على حدودها، ولكن هذا لم يفعل شيئًا يذكر لوقف المد، وأشار تقرير (الأمم المتحدة) مؤخرًا إلى أنَّ "بُطء تبادُل المعلومات والبيانات عن المقاتلين الأجانب هي واحدة من العقبات الرئيسة التي تَعترِض

التعاون الدولي لمكافحة الإرهاب"، مقدرًا أنَّ "أقلَّ من 10 في المئة من المعلومات التعريفية الأساسية على هؤلاء الأفراد قد دخلت في قواعد البيانات العالمية متعددة الأطراف".

وهذا يعني أن هناك القليل، إنْ وُجِد، من المعلومات التشغيلية المتاحة المتعلقة بالهوية، وطرق السفر، والصور، وأوامر التفتيش الدولية على سَفَر الأفراد للمشاركة في الأعمال العدائية، كان هناك تحدٍّ مماثلٌ مع الحصول على أدلَّة مادية حول نشاطات المقاتلين الأجانب التي تحدُث داخل منطقة الصراع، مما يجعل من الصعب استخدام المقاضاة كخيار أو توليد يؤدي إلى مخابرات إضافية. وصَف مسؤول كبير في الاستخبارات الأمريكية العملَ على مشكلة المقاتلين الأجانب السورية مؤخرًا بالتحدي كقضية "عَقديَّة" تُسبِّب قلقًا لمجتمع الاستخبارات.

في أعقاب هجمات باريس يناير 2015، أصبح من الواضح أن وكالات الاستخبارات الأوروبية كانت تُدقِّق في متابعة عدد كبير جدًّا من عودة المقاتلين الأجانب للخضوع إلى المراقبة، وليس هناك ما يكفي من القوى العاملة لجميع المهام المطلوبة، وللأسف عدد قليل، إن وجد، من البِلدان التي تملِك المواردَ اللازمةَ لرصد أعداد كبيرة من الأشخاص المشتبه فيهم من خلال وسائل المراقبة التقليدية، بعض التقديرات تضع تَكلفةً واسعة النطاق، على مدار الساعة، وقد تَصِل المراقبة التقليدية ضد شخص بمفرده إلى 8$ ملايين سنويًّا، قد تُمثِّل جزءًا من هذه التكلفة مجموعة إنفاق غير مُستدامة ضد آلاف المقاتلين الأجانب المتوقَّع أن يعودوا إلى بلادهم في نهاية المطاف بعد الصراعات كما هو الحال في سوريا.

هذا الواقع لا محالة سيقود الحكومات الغربية إلى الاعتماد على الجمع بين نَهْجين:

أولًا: سوف يتمُّ التوسع في استخدام إجراءات المراقبة والفحص التقني، الذي يهدف إلى جمع المزيد من المعلومات مع عدد أقل من الموارد.

ثانيًا: سيتم العمل على تطوير أساليب محسَّنة لتحليل المخاطر، وربما تطبيق التدخلات التنبؤية ضد الأشخاص المشتبه فيهم، أي من هذه الأساليب سوف تميلُ إلى تعزيز العناصر الرئيسة لنموذج الحرب الإلكترونية كما لا يزال يتعيَّن تحديد التهديدات الأمنية، والمراقبة المستهدفة بمعلومات دقيقة في الوقت

المناسب، قد اقترح اختلاف نموذج الحرب الإلكترونية بالفعل في فرنسا؛ حيث وافَق المشرِّعون مؤخرًا على إصلاح شامل لم يُسبَق له مثيلٌ من عمليات المراقبة المحلية، ممَّا يسمح الآن بجمع وتحليل البيانات الهاتفية وبيانات الإنترنت الوصفية كوسيلة من وسائل تحديد التهديدات المحتملة التي يُشكلِّها المتطرِّفون المحليون.

بجانب تهديدات الإرهاب الدولي، ظهر خطر العديد من المحللين الأمنيين بشكل مُتزايد خلال "النزاعات المختلطة" حيث تحاوِل القوات المسلحة القائمة على أساس الدولة طمسَ الإسناد العملياتي من خلال توظيف وكلاء وتكتيكات غير نظامية، كما هو الحال مع استخدام روسيا "الإنسان الأخضر الصغير" في أوكرانيا، وأبرز تقرير صدَر مؤخَّرًا عن المعهد الدولي للدراسات الاستراتيجية في إمكانية الأطراف الفاعلة غير التابعة للدول أيضًا قام باستخدام مثل هذه الأساليب المختلَطة لتحقيق مَيزةٍ غير متكافئة ضد الخصوم التقليديين.

وقد أثبتت الدولةُ الإسلاميةُ مِثلَ هذا النهج المختلَط من خلال توظيف خليط عالٍ ومنخفض من المناورة التقليدية، والتكتيكات مثل التمرد والإرهاب لتحقيق مكاسب في سوريا والعراق. شَهِدت القواتُ الفرنسيَّة في مالي تحدياتٍ مماثلةٍ في شنِّ الحملة العسكرية التقليدية ضد "العدوِّ الخفي"، حيث كان من الصعب "التمييز بين المهرَب والإرهابيِّ والمتمرِّد"، حتى التحديات المستقبلية لجيوش الدول المنافسة من المحتمل أن تلتفت إلى مَيزة الولايات المتحدة الكبيرة في الحرب التقليدية من خلال توظيف التقنيات، التي تتجنَّب المواجهة المباشرة وقناع الإسناد العملياتي، أحد المعلِّقين على تكنولوجيا الدفاع لاحَظ في الآونة الأخيرة أنَّ "الحرب آخذة في التغيُّر، سواء التي تُشنُّ من قِبل الجماعات الناشئة؛ مثل: الدولة الإسلامية أو دول مثل: روسيا."

يُشير اتِّساع مصالح الأمن العالمي للولايات المتحدة أيضًا إلى استمرار التورط في أنشطة أخرى من الحرب التقليدية ذات الكثافة العالية، مثل عمليات الاستقرار، ومكافحة القرصنة، ومكافحة الاتِّجار غير المشروع، هذه المهام تتشاركُ في العديد من الخصائص المشتركة. أولًا، أنَّها تُمثِّل الأنشطةَ التي يُسيطرُ عليها خُصومُ الشبكاتِ والأطراف الفاعلة الفردية باستخدام عدم الكشف عن الهُوية للمَيزة التشغيليَّة، ثانيًا، من المحتمَل أن تحدُث في المناطق التي تتميَّز بضعفِ الإدارة وهُويَّة الأنظمة غير الفعَّالة؛ حيث يَفتقِر جزءٌ

كبيرٌ مِن السكان إلى الوثائق الرسمية والهُوية القابلة للتحقق من هذه البعثات، مثل هذه البيئات تُعتبر مولِّداتٍ سيئةَ السمعة للفساد، وانعدام الأمن، وقضايا عدم الاستقرار التي لا يمكن الحصول عليها بسهولة من خلال استراتيجيات الرَّدْع العسكري التقليدية.

التحدي المتمثِّل في القيام بعمليات في ظلِّ أنظمةِ الهُويَّة الضعيفة لا يحظى بالتقدير بشكل عام كعامل التخطيط العسكري، قد يكونُ هذا الواجب، في جزءٍ منه، يقود إلى حقيقة أن العديد من دول العالم المتقدمة تُقيم الوظائفَ الأساسيَّة لبيروقراطية الدولة الحديثة لإدارة الهوية، يبدأ هذا الهيكل بوثائق الهُوية الأساسية؛ مثل: شَهاداتِ الميلاد ثم توسَّع ضِمن نظام الأمر الواقع للاعتمادات التي تُقرُّها الدولة، المطلوبة من أجل المشاركة الكاملة في الحياة المدنية والاقتصادية، ولكن حتى معظم الوظائف الأساسية للحكم غير موجودة في كثير من بلدان العالم، ووَفْقًا لأحد التقديرات الأخيرة، ما يصل إلى40 في المئة من الأطفال في العالم النامي لا يملكون أيَّ نوع من تسجيل الهُويَّة الرسمية عند الولادة، هذا الوضع يخلُق "فجوة الهوية" الأولية ليُصبِحوا عُرضةً للأخطاء، والفساد، والحرمان طوال الحياة.

الأهمية التشغيلية للهُوية ليست فقط مصدرَ قَلَقٍ لمكافحة الإرهاب والتمرد، ولكن أيضًا في بعثات حِفظ السلام والإغاثة الإنسانية، في عام 2014، أطلق التفويض السامي للأمم المتحدة لشؤون اللاجئين (UNHCR) أول برنامج بيومتري له في ملاوي من أجل تحسين الحماية الأمنية وتحسين توجيه المساعدة للنازحين قسرًا، وقد توسَّع هذا البرنامج مؤخَّرًا إلى جمهورية الكونغو الديمقراطية في محاولة لتحديد وتسجيل 245،000 من اللاجئين الروانديين الذين يعيشون في المنطقة و19 مخيمًا للاجئين في تشاد؛ حيث سيتم إدراج 450،000 فردٍ في القاعدة البيومترية، وسيتمُّ تحديثُ سِجلات التفويض باستخدام الاتصالات البعيدة إلى قاعدة البيانات البيومترية المركزية في جنيف، سويسرا، وفي مثال آخَرَ، الكوارث التركية وهيئة إدارة الطوارئ قامت مؤخَّرًا بتسجيل قاعدة بيومترية من 740،000 لاجئ سوريٍّ نزحوا بسبب القتال عبر الحدود، من المرجَّح أن تصبح القاعدة في عمليات الإغاثة في المستقبل والتدخلات الإنسانية في هذه البيئات مثل هذه الأدوات لإدارة الهوية.

الحرب الإلكترونية وبيئة التكنولوجيا

تطوُّر بيئة التكنولوجيا هو عامل آخَر من المرجَّح أن يحول العلاقة بين الأمن والهوية والحرب، وطرحتْ باحثة الأمن القومي روزا بروكس مؤخَّرًا مسألة الكيفيَّة التي سيتمُّ بها تغيير الحرب في هذا العصر عندما نعرف عدونا بالاسم، من وجه، وحتى الحمض النووي، وهي تُلاحِظ أنه في الصراعات الأخيرة، قد عرفتِ الولايات المتحدة الكثيرَ عن خصومها، "بين المخبرين البشريين ومراقبة التكنولوجيا الفائقة، ونحن غالبًا نعرف أين ولدوا، حيث ذهبوا إلى المدارس والجامعات، وأسماء أشقائهم والأطفال، التسلية المفضلة لديهم، وأكثر من ذلك بكثير".

بروكس وغيرهم مثل باحث القانون العسكري تشارلز دنلاب الذي قام بالتكهن حول مستقبل ليس ببعيد، حيث الأسلحة فائقة الدقة المتقدمة مع برنامج التعرف على الوجه سوف يتجوَّل في "ساحات القتال بحثًا عن قوة العدو"، ورغم أن هذا السيناريو قد لا يكون الآن حقيقة واقعة، إلا أن عِدَّة اتجاهات من تكنولوجيا المعلومات تدفع بالفعل الحرب الإلكترونية في هذا الإتجاه.

من المرجَّح أن يغيب عن البال كعهد العقد المقبل عندما أصبحت التقنيات الحيوية طبيعية، وتم دمجُها تقريبًا مع كلِّ جانب من جوانب الحياة اليوميَّة. كانت قطاعات الدفاع والأمن وإنفاذ القانون أوَّلَ مَن أَدرَك قيمة القياسات الحيوية للتطبيقات مثل مراقبة الحدود، والوصول إلى النُّظُم، والتحقق من الهُويَّة. تحديد هذه المتطلّبات إلى حدٍّ كبير يهتمُّ بالتركيز الأَوْليِّ للبحث والتطوير في هذا المجال، فضلًا عن كيفية تطوُّر هذه الأدوات؛ ومع ذلك، تتغيَّر هذه الديناميكية يتغيَّر، القطاع الصناعي الخاص يتسابَق بالفعل قبل الحكومات في استخدام التقنيات الحيوية، وخاصة في مجالات الإلكترونيات الاستهلاكية الشخصية وأدوات أمن المعلومات.

وهذا يعني أن الحكومات من المرجَّح أن تتخلَّف عن الركب من حيث التأثير على اتجاه الابتكار على نحو مُتزايد، وقد أَعْرب خبراء الصناعة عن المخاوف من غياب التخطيط والتنسيق بين الجهات الحكومية المناسبة، وبين الشركاء الدوليين، وكذلك تقليل الدور الذي تلعبه الحكومات في تحديد مستقبل هذه الصناعة، ومن المحتمل أن تخرُج من القطاع التِّجاري، إلا إذا تمَّ استغلالُها من قِبل مصالح الأمن وتقنية اختراقات الدفاع الجديدة، في بعض الحالات، سيتمُّ تطبيق موقف ردِّ الفعل إلى مسائل الحكم ووضع القواعد، وخصوصًا الابتكار التكنولوجي الذي يفوق قُدْرَةَ الدولة على تحديد سياق استخدامه.

هذا الوضعُ هو التحوُّل الدراماتيكي من نموذج عصرِ الحربِ الباردة إلى المجسَّات المتطوِّرة وأنظمة جَمْع المعلومات الاستخبارية التي تطوَّرت من خلال البحث والتطوير الذي ترعاه الحكومةُ، وهذا له عِدَّة آثارٌ هامة. أولًا، في بعض المجالات التقنية للحرب الإلكترونية، فإنَّ الولايات المتَّحِدة تجِد نفسَها في حالة من التكافؤ التكنولوجي مع الخصوم المحتملين، سواء الجهات الحكومية أو غير ذلك.

ثانيًا، من أجل تقليل الفجوة التكنولوجية، سيَتعيَّن على حكومة الولايات المتحدة تسويةُ الكثير من النواقص التي طال أمدُها في عملية الشراء من أجل البقاء بالقرب من الحافة الأمامية مع تطوُّر التكنولوجيات الجديدة.

تتوقَّع مُنظَّمة البحوثِ الصناعية أنه بحلول نهاية عام 2015، سيكون هناك 619.000.000 يقومون باستخدام القياسات الحيوية على أجهزتهم المحمولة، بما في ذلك بصمات الأصابع والصوت وقزحية العين، الوجه، وطرائق مختلفة من القياسات الحيوية السلوكية. وتُشير تقديرات أخرى إلى أن أكثر من مليار شخص في البلدان النامية قد سجَّل بالفعل شكلًا من أشكال التوقيع البيومتري من خلال تَفاعله مع الأجهزة الإلكترونية الاستهلاكية، والمؤسسات المالية، والحكومات المحلية. بالإضافة إلى ذلك، فإن نِقاط الضعف الكامنة في الأساليب التقليدية للمصادقة الشخصية (على سبيل المثال، كلمات السر) هي التي تقود نموَّ القطاع التِّجاري الكبير لتحسين طرق إدارة الهُوية.

وبعيدًا عن التطبيقاتِ التِّجارية، فإن العشرات مِن الحكومات يُتابعون مشاريع جوازات السفر الإلكترونية والتأشيرات، وسجلات الناخبين، ورواتب القطاع العام، والرعاية الصحية، وبرامج تقديم الخدمات الاجتماعية وتحديد التمكين البيومتري (ID)، وقد تتجنَّب بعض الحكومات نِظامَ الهُوية الورقية، وتنتقل مباشرة إلى تكنولوجيات التمكين البيومتري، والجدير بالذِّكر أن الهند، مع عدد سكانها فأنهم لا يحملون وثائقَ ضخمة، وتعمل حاليًّا خلال عدة سنوات من التخليص البيومتري فقط لمليار من السكان كجزء من نظام التحديد الوطني الجديد. وسيتم ربط الصفات البيولوجية لعدد من الهُوية الفريدة من نوعها واستخدامها لوظائف مِثل إدارة الإعانات التي تُقدِّمها الحكومة ومراقبة توزيع الحِصص الغذائية.

وكمثال آخر، وزارة الداخلية للمملكة المتحدة (UK) أدخلت مؤخرًا "تصريح الإقامة البيومترية" الذي مِن شأنه أنْ يكون من أجل حاجة أيٍّ من الرعايا الأجانب من خارج المنطقة الاقتصادية الأوروبية الذين يرغبون في العمل أو الدراسة في المملكة المتحدة، ينبغي على حامل البطاقة تقديم أوراق الاعتماد على الحدود عند السفر داخل أو خارج المملكة المتحدة. التطبيقات الجديدة الأخرى آخذة في الظهور كل يوم مثل استخدام كينيا للبطاقات البيومترية لضمان أن الموظفين العموميين يظهرون للعمل والتشريعات، قامت نيجيريا مؤخرًا بتكليف التسجيل البيومتري من بطاقات التعريف المشترك للهواتف المحمولة(SIM)؛ بحيث يمكن للحكومة أن تَتَّبع الأنشطة غير المشروعة. تليها باكستان التي دعتْ مؤخَّرًا إلى تسجيل بطاقاتSIM البيومترية بعد أن تبيَّن أن جميع المهاجمين الستة الرئيسين في هجوم ديسمبر 2014 على المدرسة العسكرية كانوا يستخدمون الهواتف المحمولة المسجَّلة لامرأة واحدة مع عدم وجود صِلة واضحة للمهاجمين.

تَتسارَع وتيرة الابتكار في إثارة المخاوف بشأن الخصوصية والمراقبة. بالإضافة إلى ذلك، من المحتمل أن تكون القضايا الصعبة مع المخاوف التنظيمية والحكم وكذلك الصراعات على المستوى الفني، التوافقي، وتكامل البيانات.

ولعلَّ الأهم من ذلك، أن الكثير من التطوير في هذا المجال من المحتمل أن يكون خارج سيطرة الدولة الواضحة. ويمكن للحكومات، وخدمات الأمن، والقوات المسلحة أن تجد نفسَها في موقف الحَكم المحتجز، بدلًا من صناع الحكم عندما يتعلَّق الأمر بتحديد كيف تَزدهِر التكنولوجيا، ويتم استخدامُها من قِبل الجمهور العام. القياسات الحيوية هي مجرَّد مثال واحدٍ لهذا الإتجاه العام بشأن الابتكار التكنولوجي في عصر الحرب الإلكترونية. تَنطبِق الدينامية المماثلة إلى مجال الإنترنت أيضًا.

في النزاعات الأخيرة أصبح عدم الكشف عن الهوية مركزًا للأهمية المتزايدة لجاذبية الجِهات الفاعلة غير التابعة للدول، وفي بعض الحالات، ينبغي على الجهات الحكومية محاولة تجنُّب العمليات الإسنادية. يمكن أن توفِّر الهويات المحمية معرفةَ هذه الخصوم مع المرونة، والتنقل، والاستفادة من المفاجأة. عدم الكشف عن الهوية يسمح بسلامته في مجال الاتصالات، والتوظيف، والتمويل، والتخطيط، وكذلك شَكْل التمويه من خلال شنِّ حرب المعلومات. ويُقدِّم مجال الإنترنت للخصوم منطقةَ الحرم النسبي؛ حيث الهويات الحقيقية يمكن أن تكون محمية، مخفية، أو متلاعَب بها. ويمكن للجهات الفاعلة أن تخفي الأنشطةَ وراء التشفير القوي، التجسيد الرقمي، أو الأدوات الفنية التي تعقد الإسناد وإحباط المراقبة.

وأشارت الاستراتيجية الإلكترونية المحدَثة مؤخرًا لوزارة الدفاع إلى كيفية اعتبار عدم الكشف عن الهُوية على شبكة الإنترنت، هو تمكين مباشر للنشاط الإلكتروني الخبيث من قِبل الدولة والجماعات غير التابعة للدول. كانتِ الدولُ الإسلامية في العراق وسوريا (ISIS) واحدةً مِن أكثرِ الأمثلةِ البارزة على هذا الإتجاه. وكان آخرُ استخدام لروسيا "المتصيدون" الإنترنت لتوليد الدعاية المؤيدة للنظام التي تهدُف إلى التأثير على بيئة المعلومات المتعلِّقة بالعمليات في أوكرانيا. فصَّلت الدراسةُ الحديثة كيف يتوقَّع أن يُسجِّل 50 مقالة إخبارية يوميًّا، والحفاظ على العديد من حسابات الفيسبوك وتويتر، وتوليد عشرات المشاركات في اليوم الواحد، البالغة حوالي 40،000 من التعليقات على الإنترنت كلّ يوم لدعم العمليات الإعلامية الموالية للكرملين "المتصيدون" المجهولة.

تَقديرًا لهذه التحديات الجديدة، فإنَّ استراتيجية وزارة الدفاع تدعو على وجه التحديد إلى "أن قدرات الاستخبارات تُساعد على كشف الشخصية السيبرانية الفاعلة، وتحديد نقطة الهجوم في المنشأ، وتحديد التكتيكات والتقنيات والإجراءات" مِن أجل دعم الردع، ردًّا على ذلك، وإنكار العمليات.

وكان الرئيس الاستوني توماس هندريك إلفيس مفكرًا رائدًا في قضايا الدفاع السيبراني، وأشار مؤخرًا إلى كيفية تُقارب الجريمة المنظمة والشبكات الإرهابية، والجهات الحكومية بسرعة في هذا المجال، مما يجعل من الصعب على الجهات الفاعلة المشروعة التمييز بينهما. كان تحدي الهوية والإسناد في مجال الإنترنت هو ساحة عمليات الحرب الافتراضية لـ"مرحلة الصفر"، وهذه الأنشطة تهدُف إلى تشكيل المفاهيم وتأثير السلوك تمهيدًا للعمل الحركي. وشُوهِدت الأمثلة الأخيرة قبل التدخلات العسكرية الروسية في جورجيا وأوكرانيا.

وعلى نِطاق أوسع، يُوفِّر نِطاق الإنترنت مكانًا للتأثير على السلوك وتشكيل النتائج من خلال الأنشطة القصيرة للاشتباك العسكري التقليدي. يَنْطوي هذا النهج على مخاطر مادية أقلّ للخصوم بتقديم قُدرةٍ أكبر على إخفاء هُويَّاتهم من خلال الأدوات التِّقنية المتاحة بسهولة. هذه الخصائص تجعل المجالَ الإلكتروني مريبًا إلى حد كبيرٍ في عصر الحرب الإلكترونية. العديد من التقنيات الممكنة في هذا المجال، هي ديمقراطية وقابلة للغاية، وهذا يعني أنه، خلافًا للأسلحة الأقوى لِحقبة الحرب الباردة، إلا أن أسلحة المجال الإلكتروني عادة ما تكون في متناول أي شخص لديه المهارات اللازمة والأدوات الأساسية. لهذا السبب، يَعرِض الإنترنت منصَّة منطقيَّة للأطراف الفاعلة غير التابعة للدول التي تسعى لتوظيف قُدرات غير متكافئة ضد الدول مع تجنُّب الإسناد المباشر.

المجموعة المتنوِّعة من الأدوات التي يَسهُل الوصول إليها يمكن أن توفِّر للمستخدمين الشبكات المتوازية التي تم تشفيرها، اللامركزية، وإلى حد ما، المجهول. "سيلك رود" المعروف على الإنترنت باسم "شبكة الإنترنت المظلمة" هو موقع تجاري أُغلِق مؤخرًا من قِبل مكتب التحقيقات الفدرالي هو مثال على ذلك.

تعتمد الجِهات الفاعلة الأخرى على الأدوات، مثل شبكة تور، التي تُوفِّر الحماية ضد تحليل حركة المرور والمراقبة من قبل إخفاء بروتوكول الإنترنت (IP) للعناوين ومواقع الخادم أثناء تشفير حزم البيانات وتوجيهها من خلال العقد المتعددة، مما يجعل من الصعب تعقُّب وتحديد المستخدمين. ويُقدِّر بعض الخبراء أنَّ هذه المواقع المظلِمة تمثِّل جزءًا كبيرًا من النشاط على شبكة الإنترنت، والتي تنطوي على محتوى لا تتم فهرستُه ويتم اكتشافه عن طريق محركات البحث التقليدية مثل جوجل. بالإضافة إلى ذلك، يمكن "التشفير–العملات" الرقمي مِثل بيتكوين فهو يُوفِّر وسيلة لإجراء المعاملات المالية تحت اسم مُستعار عَبْر هذه الشبكات. عدم الكشف عن الهُوية يمكن المستخدمين من التصفح، والتواصل، وتجارة المواد غير المشروعة مع خطر أقل عمومًا من كَشف الهوية وزيادة القدرة على إخفاء المواقع المادية والهوية.

هناك بالفعل اقتراح بأنَّ الدولة الإسلامية وغيرها من الجماعات المتطرِّفة تَستخدِم مِثلَ هذه الأساليب. ولاحَظ رئيس شبكة مكافحة الجرائم المالية التابعة لوزارة الخزانة الأمريكية مؤخرًا أن "عند بَدء الحديث عن المعاملات العالمية من نقطة إلى نقطة والحركة اللحظية للقيمة على الحدود، التي لديها مخاطر حقيقية مرتبِطة به." مدير وكالة الأمن القومي الأميرال مايكل روجرز شرح بشكل أكثر وضوحًا هذه المخاطر، مشيرًا إلى أن وكالته تراقِب التهديدات على شبكة الإنترنت المظلِمة حيث يقضي "الكثير من الوقت يتَّبع الناس التي لا يمكن العثور عليها."

استخدام مواقع مجهولة "الشبكات المظلمة" لافتٌ للنظر خاصَّة في مقابل الارتفاع المتزامن لوسائل الإعلام الاجتماعية، والظواهر على أساس المفهوم على عكس الهدف لإسقاط الهوية لغرض صريح بناء على أساس الانتماء. بالنسبة لكثير من الجماعات، أصبحت أنظمة وسائل الإعلام الاجتماعية الأداة المفضلة لتواصل توزيعها، والتخطيط، والتوظيف، ونشر الدعاية، بما في ذلك الجماعات الإرهابية، والمتمردين، والمنظمات الإجرامية. وصَف تقرير الإتجاهات العالمية لمجلس الاستخبارات الوطنية مؤخرًا هذه التقنيات للتواصل الاجتماعي مثل "طبيعتها المقاومة للرقابة المركزية والتحكم"، مع احتمال أن تحلَّ محلَّ مصادر الطاقة التقليدية والسلطات لصالح الأفراد والجماعات الصغيرة، والتحالفات المؤقتة من الجهات الفاعلة غير التابعة للدول.

العديد من الأمثلة الأخيرة تدل على الدرجة التي تطوَّرت بها وسائل الإعلام الاجتماعية كأداة تنفيذية، الجماعات المسلحة في غزة، والخلايا الإرهابية في مالي، وتجار النفط في نيجيريا، والقراصنة في سواحل الصومال قد استخدموا كل وسائل الإعلام الاجتماعية؛ مثل: شبكات القيادة والسيطرة المخصصة لإجراء عمليات المعلومات. الدولة الإسلامية، على وجه الخصوص، قد وضعت وجودًا رقميًّا قويًّا ومتطورًا، وتم نشر محتوى الوسائط عالية الجودة عبر الأنظمة المتعددة في الوقت المناسب." صدر تقرير مؤخرًا عن الإرهاب وتم العثور على الوسائط الجديدة حوالي 90 في المئة من الأنشطة الإرهابية التي تقوم باستخدام الإنترنت ووسائل الإعلام الاجتماعية باعتبارها أداة تواصُل، في بعض الحالات تم تقديم "جدار الحماية الظاهري للمساعدة في الحفاظ على هوية أولئك الذين يشاركون."

وقد وصف مديرNSA في بريطانيا العظمى، مقرَّ الاتصالات الحكومية (GCHQ)، تويتر، الفيسبوك، والواتس آب باسم " شبكات القيادة والسيطرة كخيار للإرهابيين والمجرمين." اقْتَرح أحد المعلقين على التكنولوجيا العسكرية أنَّ الوضع والوعي في عصر الإنترنت يعني استخدام "البيانات اللحظيَّة من الشبكات الاجتماعية؛ مثل: تويتر والفيسبوك لتحديد الهدف." في حين أن المبالغة والتعليق لا يشيران إلى أي مدى أصبحت هذه الأنظمة مكونًا هامًّا من مكونات البيئة التشغيلية المعاصرة.

ربما يوفِّر الصراع السوري المثالَ الأقوى لكيف أصبحت وسائل الإعلام الاجتماعية أداة من أدوات الحرب الحديثة. وقد دعا هذا الصراع "الصراع المدني الأكثر اجتماعية في التاريخ" مع المقاتلين باستخدام الفيسبوك، يوتيوب، تويتر، وسناب شات لمجموعة متنوعة من المهام التنفيذية، والاتصالات، والدعاية. حدَّد تحليل في أواخر عام 2014 حوالي 46،000 على الأقل من حسابات تويتر المستخدمة من قِبل أعضاء وأنصار الدولة الإسلامية، في حين تشير تقديرات مكتب التحقيقات الفيدرالي أن حوالي200،000 شخص في جميع أنحاء العالم يَصِل إليهم "الرسائل الإرهابية" كل يوم عبر وسائل الإعلام، وأشرطة الفيديو، كتيبات التعليمات الاجتماعية، وغيرها من المواد المنشورة على المواقع الإسلامية المتشددة.

كما استُخدِمت هذه الأنظمة على نِطاق واسع لنَشْر المعلومات التشغيلية والتوظيف، وأغراض التدريب. على سبيل المثال، نشرتِ المواقعُ مَعلوماتٍ حول استخدام المتفجِّرات وتقنيات القتال، وروابط برامج التشفير المصمَّمة لمساعدة المستخدمين على حماية الاتصالات الحسَّاسة. يُستخدَم أيضًا المقاتلين الفرديين الحسابات الشخصية لإنشاء نواياهم الحسنة وتوثيق الخبرات القتالية مباشرة. في مثال واضح، حاول أحد مقاتلي الشباب البريطاني بيان وهمية ساحة المعركة على وسائل الإعلام الاجتماعية بعد وضعه على قائمة مراقبة السفر. في نهاية المطاف تم القبض عليه عند محاولة الدخول مرة أخرى إلى المملكة المتحدة. وقد سُلِّط الضوءُ على سبيل المثال إلى أي مدى تستفيد العديد من الجهات الفاعلة غير التابعة للدول من وسائل الإعلام الاجتماعية لصياغة الهويات المشروعة إلى الجمهور الخارجي.

ومع ذلك، يمكن أنْ يكون النشاط على الإنترنت سلاحًا ذا حدَّين، وكلاهما يمكن عمليات الخصم، بينما في الوقت نفسه يعرِّضهم إلى المراقبة. في السنوات الأخيرة، تم عرض استغلال وسائل الإعلام الاجتماعية وتعمُّق الطب الشرعي الرقميّ في عمليات الخِصْم. فعلى سبيل المثال، في أوائل عام 2014 كان المحللون قادرين على تعقُّب تحركات أفراد الجيش الروسي في شبه جزيرة القرم من خلال وسائل الإعلام الاجتماعية. بشكل مُنفصِل، قدَّمتْ أشرطة فيديو يوتيوب ورسائل تويتر بواسطة الجهات غير النظامية الروسية التلميحات الأولى لمسؤوليتها عن إسقاط رحلة ماليزيا إيرلاينز ال 17 في شرق أوكرانيا في يوليو 2014. وفي الآونة الأخيرة، أثبت "حجم المصادر" أن المعلومات التي تُنشَر على وسائل الإعلام الاجتماعية من قِبل السكان المحليين لها دور روسي نَشِط في شرق أوكرانيا، بما في ذلك التدفق المستمر من الأسلحة والقوات، وحتى تستمرَّ الحكومة في نفي أي تورُّط مباشر في الأعمال العدائية.

في سوريا، تم ذِكر أن القوات الموالية للأسد تستخدمُ التجسد الوهمي على الإنترنت لتحديد واستهداف أعضاء المعارضة. واستخدم الباحثون هذه الهويات الوهمية للحصول على معلومات شخصية مفصَّلة، بما في ذلك الأسماء وأماكن أعضاء أحزاب المعارضة والنشطاء والإعلاميين والعاملين في مجال المساعدات الإنسانية، واعتبر البعض الآخر خطرًا على النظام. وكشفت حسابات سكايب والتطبيقات النقالة (التطبيقات)، ومواقع وسائل الإعلام الاجتماعية العناوين وسجلات الرسائل القصيرة، والبريد الإلكتروني، وغيرها من المعلومات المتعلِّقة بخطط القوة المعارضة.

ووفقًا للتقييم، فقد أنتج هذا النوع من الاستغلال وسائلَ الإعلام الاجتماعية العدوانية "المخابرات العسكرية لتنفيذ مَيزة المعركة المباشرة،" بما في ذلك تمكين تلك المعلومات القوات الموالية للأسد من تحديد المسار، واستهداف أعضاء المعارضة الرئيسين.

إن الولايات المتحدة قامت أيضًا باستخدام بيانات وسائل الإعلام الاجتماعية للاستهداف. فقد كَشَف مسؤول عسكري في الآونة الأخيرة أنَّ مشاركات وسائل الإعلام الاجتماعية في الآونة الأخيرة قد تمَّ استخدامها لتعقُّب وضرب مبنى مقرِّ جماعة الدولة الإسلامية في وقت لاحق، واستخدم الباحثون غيرها من الوسائط الاجتماعية باعتبارها وسيلة لبناء الملامح الديمغرافية لمقاتلي الدولة الإسلامية وغيرهم من الجماعات، وتسليط الضوء على مواقعها، ما اللغات التي يتحدثون بها، وكيفية الوصول إلى الإنترنت، وتحليل مضمون اتصالاتهم؟

وفي تطوُّر آخر استطاعتِ الشبكة الدولية للإنترنت من "كِيانات النِّضال البرمجيِّ" المعروف باسم مجهول مؤخرًا السيطرة على حسابات تويتر والفيسبوك التي تستخدمها الدولة الإسلامية وتهديد أعضاء المجموعة "بمطاردتهم، إنزال المواقع الخاصة بهم وحساباتهم ورسائل البريد الإلكتروني، وأنه مِن الآن فصاعدًا، لا يوجد مكان آمن بالنسبة لهم على الإنترنت". ووَفْقًا لأحد الخبراء، إن "استغلال الشبكة الآن جزءًا روتينيًّا في التكنولوجيا المنخفضة، والحروب الأهلية، ومتاحة لتلك التي تعمل على ميزانية صغيرة."

تَعرِض كثافة المعلومات في مجال الإنترنت بوضوح التزاماتِ "الأمن غير التشغيلي الواعي (non-OPSEC) بأنَّ توظيف مجتمع المقاتلين الأجانب يوفِّر نافذةَ الاتصالات على الهُويَّات والأنشطة. ويَستنِد تصميم شبكات وسائل الإعلام الاجتماعية على تسلسل الاتصال والروابط الترابطية بين الأفراد. وغالبًا ما يتمُّ تعزيز هذه المعلومات عن طريق بيانات غَنيَّة المحتوى، بما في ذلك الصور والنصوص والفيديو، والصوت، مع وضْع علامات تحديد الموقع الجغرافي والطوابع الزمنية.

ويمكن أيضًا أنْ تستمدَّ بعض التوقيعات البيومترية السلوكية من هذه الأنشطة الرقمية الروتينية التي تظهر أنماطًا في كيفية نَشْر المعلومات واستخدام أجهزتهم، وكثير من الخبراءِ في هذا المجال يَجهلون مَصدرَ الوجود الرقمي السهل نسبيًّا، لنزع المصدر عن طريق الربط بين قواعد البيانات المتاحة للجمهور، معلومات بطاقة الائتمان، وسِجلَّات الناخبين، والعلاقات الشخصية، وأنماط المعلومات السلوكية الكافية لتجميع الملفات الفردية العالية لمعظم مستخدمي الإنترنت بشكل عام، ويوفِّر هذا العرضُ أداة قوية لمخططات تكوين الشبكة وتحديد الأفراد الذين يعملون داخلها، التي تدعو إلى مقولة يوهان غوته، "قل لي: من رفيقك، وأنا أقول لكَ من أنتَ."

وقد اقترح الباحث القانوني والجنرال المتقاعد تشارلز دنلاب أنَّ تَوفير توسيع "البيانات الكبيرة" والأدوات الإلكترونية الجديدة قد يُمكِّن "الإفراط في تخصيص الحرب،" مما يؤدِّي إلى استهداف صريح لأفراد معينين داخل وخارج ساحة المعركة. ولاحظ دنلاب "عددًا لا نهائي تقريبًا من السيناريوهات التي تمكن الخصوم من الإفراط في تخصيص الصراع عبر الوسائل الإلكترونية"، وهذا الوضع المستقبلي للحرب قد سبق حدوثه، والذى تجسَّد مؤخرًا في اختراق أنظمة الكمبيوتر في مكتب إدارة شؤون الموظفين، واالقرصنة الصينية المرتبطة بالوزارة الشعبية، وثالثًا المجموعة السيبرانية المكلَّفة لجمع الاستخبارات العسكرية، وركَّزت هذه القرصنة تحديدًا على البيانات الشخصية والعمل والتاريخ الطبي للآلاف من الموظفين الحكوميين والعاملين في الجيش والاستخبارات، ومقاولي الدفاع، بما في ذلك معلومات عن الأصدقاء وأفراد العائلة والزملاء المستمدَّة من نماذج التصريح الأمني.

وقد وجّه الاهتمام إلى تطوُّر زيادة توافُر البيانات مفتوحة المصدر ومحتوى الوسائط الاجتماعية والديمقراطية للاستخبارات، فخلال حِقبة الحرب الباردة، تم استخدام الأنظمة الأساسية لجَمع التقنية المتقدمة الذي اقتَصر على حَفْنة من القوى العسكرية الكبرى، ومع ذلك، فإنَّه في عصر الحرب الإلكترونية، المجموعات الصغيرة، والكِيانات التِّجارية، وحتى الجهات الفردية كان لديهم القدرة على جَمع المعلومات بشكل مُستقلٍّ واستخدامها لمجموعة متنوعة من الأغراض، قد جمع تجُّار التجزئة معلومات مفصَّلة بشكلٍ رُوتيني حول عادات الإنفاق وتاريخه الائتماني وتاريخ تصفُّح شبكة الإنترنت، وظائف الشبكة الاجتماعية، والمعلومات الديموغرافية لأبحاث السوق والإعلانات المستهدَفة على وجه التحديد.

وقد استُخدِمت أساليبُ مماثلةٌ من قِبل محلِّلي الاستخبارات المستقلين؛ لافتة للنظر في عام 2013؛ حيث استخدم مُدوِّن من إنجلترا مصادرَ وسائلِ الإعلام الاجتماعية لإثبات تقارير الحكومة السورية، باستخدام الأسلحة الكيميائية ضد أهداف المعارضة في إحدى ضواحي دمشق، وأكد المدون نفسه في وقت لاحق على تقارير تُفيد بأن الجيش السوري الحر قد حَصل على مدافع مضادَّة للطائرات، وكان قادرًا على تتبُّع التقدم التكتيكي للمتمردين السوريين وتفاصيل تطويرهم للأسلحة البدائية عن كَثَب، وفي حديث آخر عن "حجم مصادر" الاستخبارات المستمدَّة من وظيفة وسائل الإعلام الاجتماعية المضاف إليها علامات جغرافية تحتوي على صور من المركبات العسكرية الروسية التي تتحرَّك عَبْر أوكرانيا، وقد أصبح هذا قاعدة بيانات متزايدة، وضعت تمامًا من التقارير المستخدمة المجمَّعة حول الأنظمة التجارية، القائمة الظاهرية من الغارات التي تَشُنُّها القوات الروسية والمعدات وانتهاكات وقْف إطلاق النار.

وعلى الرغم من القيمة الواضحة لهذه الأدوات، هناك تحديات كبيرة في استخدام الكثير من المحتوى، الذي تم الحصول عليه من وسائل الإعلام الاجتماعية والمحتوى المقدَّم من المستخدمين، ومن وجهة نظر تحليلية، هناك مهمة صعبة تتمثَّل في تصفية البيانات التي يمكن أن تكونَ مفيدة لكمية هائلة من الفوضى الرقمية، والضوضاء، والتضليل، والمسألة الثانية: هي واحدة من الإسناد، مع العلم بتحديد هُوية الفرد وراء المعلومات، كالكرتون الكلاسيكي نيويوركر لاحظ نبويا في عام 1993، "على شبكة الإنترنت، أنه لا أحد يعرف أنه كلب"، وخلافًا مع القياسات الحيوية، على الإنترنت يتم إنشاء الهويات الرقمية، التي لا تورث، ويُشار إلى هذا في وقت ما على أنهم "أشخاص الإنترنت "ويمثِّل كيف يتمُّ التعرف على مُستخدِمِ الشبكةِ الواسعةِ من خلال الصِّفات الرقمية؛ مثل: عُنوان البريد الإلكتروني، وعنوانIP الخاص بالكمبيوتر، أو رقم الهاتف الخليوي، ومع ذلك، هذه الهُويات يمكن هندستُها، أخفاؤها، والتلاعب بها لأغراض محددة.

قام معظم مستخدمي وسائل الإعلام الاجتماعية بممارسة ما لا يقلُّ عن بعض أشكال الأمن التشغيلي، في حين أنَّ كثيرين غيرهم يعملون عمدًا وراء قناع من الهُوية الوهمية والخداع، فالفضاء الإلكتروني مليء بالحسابات الوهمية على تويتر، والرقمية، واستخدام برامج إخفاء الهوية، وتَنصح المنتديات الجهادية الآن المشاركين باستخدام إجراءات متطوِّرة لتجنُّب الكشف عند التصفح، بما في ذلك خطوات لإزالة تحديد

الموقع الجغرافي والبيانات الوصفية من صور الهاتف الخليوي، على نحو متزايد، قامت العمليات التشغيلية (OPSEC) المتشدِّدة أيضًا باستخدام تطبيقات الرسائل المشفرة مثل ال (WhatsApp) & (KIK)، أو التطبيقات التي تدمِّر البيانات مِثل (Wickr) & (Surespot) التي تجعل من الصعب جدًّا على السلطات الشرعية تحديد الفاعلين وتتبُّع اتصالاتهم، هذا الكم الهائل من الخداع والتضليل في مجال الإنترنت خلق صناعة منزلية من الشركات المتخصِّصة في التحقق من تقارير وسائل الإعلام الاجتماعية باستخدام المعلومات الجغرافية؛ مثل: التتبع، التحليل، والكلام، وتحليل المحتوى لتحديد الدجالين والهويات الوهمية.

ويَكمُن التحدي بالنسبة للقائمين على المشروع؛ في كيفية ربْط الشخصية الإلكترونية إلى الهُوية الحقيقية للفرد فيما وراء الوجود الرقميِّ، كما أشار أحد خبراء الترميز والتشفير الأمنيِّ في الآونة الأخيرة، قائلًا: "نحن نعيش في عالم لا يُمكِن أن نحدِّد فيه بسهولة الفرق بين اثنين من الأشخاص في شقة بالطابق السفلي وبين حكومة كوريا الشمالية" وهو ما خَلَق في الواقع "سباق التسلح بين المهاجمين، وبين من يستهدفون التعرف إلى هؤلاء"، وردًّا على هذه التحديات، كانت وكالة الاستخبارات المركزية (CIA) بصدد القيام بعملية إعادة هيكلة واسعة تَستنِد في جزء منها على إدراك أن هذه البيئة الجديدة قد تتغيَّر بشكل جَذريٍّ حول التجسس، وكجزء من هذا النهج الجديد، يَزيد تنظيمُ التقارير من مهارات الشبكات الرقمية عبر كلِّ فئة من العمليات، على سبيل المثال، استخدام الأدوات الإلكترونية من أجل "تأكيد الهويات بهدف ضربات الطائرات بدون طيار أو اختراق الخصم في الإنترنت والدهاء مثل الدولة الإسلامية".

فكلُّ هذه القضايا ترتبِط مباشرة بالعناصر الأساسية لنموذج الحرب الإلكترونية، الفردية، والهوية، والمعلومات، كما استهدف فحص الشخصية على أساس الهُوية التي تصبح طبيعية، فإنَّ قضية الهوية والإسناد تنمو فقط باعتبارها قلقًا تشغيليًّا؛ لهذا السبب، من المهم أيضًا النظر في كيفية تغيُّر مفهوم الهُوية نفسه في المستقبل.

مفهوم الهوية يمكن أن يكون محبطًا، لا سيما بالمقارنة مع أكثر الجوانب الملموسة لاستراتيجية الأمن القومي والحرب، ويمكن القول، معنى الهوية أثناء التحول الثوري، مع التغييرات بلا شك سيكون لها آثار كبيرة على كيفية شنِّ الحرب الإلكترونية في المستقبل، هذا القسم يُعتبر لفترة وجيزة يُقدِّم مضاربات على الإتجاهات الاجتماعية والاقتصادية والتقنية، التي من المرجّح أن تشكِّل معنى الهُويَّة: من حيث صِلتها بتحديات الأمن القومي في المستقبل.

كما افترضت هذه الدراسة، أن الهوية قد أصبحت في إطار نموذج الحرب الإلكترونية في "مركز الجاذبية" التشغيلي للخصوم الشبكية، والأطراف الفاعلة غير التابعة للدول، والمقاتلين الفرديين، كما تَصوَّر كارل فون كلاوزفيتز، أنَّها تمثِّل "محورَ كلٍّ من القوة والحركة، والتي تُوقِف كل شيء"، ففي الصراعات التقليدية، فهذا يشير عمومًا إلى القدرات العسكرية للعدو، تلك الأصول والصفات التي تمكِّنها من تطبيق القوة القتالية على ساحة المعركة، في حالة الحرب غير النظامية وحركات التمرد، ومركز الجاذبية يُنظَر إليهم عمومًا من الناحية الشرعية السياسية، والعوامل الأمنية، والقدرة على ممارسة الضغط على السكان؛ لأنها تمثِّل في جوهرها مصدرَ للقوة، وكذلك ضعفها وهشاشتها، في عصر الحرب الإلكترونية، أصبحتْ مركزَ جاذبية جديد للهوية.

وتماسُك الشبكةِ يأتي من الهُوية والعلاقات الترابطية بين أعضائها، الهوية هي التي تميِّز الشبكات الاجتماعية من البيروقراطية، في حين أنَّ البيروقراطية مسلوبة الشخصية، وتعمل على الأساس الداخلي والبروتوكول، وتستمدُّ الشبكات الاجتماعية قوَّتَها من الاتصالات الشخصية، والثقة، والتوقعات التي يُنظَر إليها بدلًا مِن التوقعات المقنَّنة، وسلامة شبكة الخَصم تعتمِد على الثِّقة بالهويات المحمية التي يُمكِن

الوثوقُ بها داخليًّا وخارجيًّا، ونفي عدم الكشف عن الهوية لشبكة العدو ليحرمه من قوة فريدة من نوعها، مع تحديد العناصر، تتعرَّض الاتصالات، والأنشطة، والشبكة إلى أن تصبح ضعيفة، مع هذا التعرض، فإنه يَفقِد القدرةَ على العمل، للمناورة، للتخطيط، والتواصل.

طبقًا إلى التماسك الشبكيّ، فمن المهم أن نفهم كيف يتغيَّر مفهوم الهُوية. العديد من هذه التحولات هي نتيجة لأحدث ابتكارات التقنية التي تُغيِّر كيفية إنشاء معلومات الهُوية وتخزينها وتبادُلها، والتحقق منها، بالإضافة إلى ذلك، العوامل الاجتماعية التي تُسبِّب تآكل الوظيفة التقليدية للدولة باعتبارها السلطة الوحيدة لإرجاع الهوية الرسمية، فعلى الأفراد وكذلك الشركات أن يأخذوا زمام المبادرة في تحديد مفاهيم الهُوية الجديدة وخلق إطار لكيفية استخدامها، وتلعب القوى الاقتصادية أيضًا دورًا، مثل التخصيص التجاري ونمو "تقاسم الاقتصاد"، نعرض آليات هذه التغييرات الجديدة للتحقق من الهوية، إسناد المعاملات، والأهمية المتزايدة المفروضة على مصلحة السمعة. ونتيجة لذلك، تتطوَّر أشكال جديدة من الهُوية الرقميَّة مِن أجل التحقق من الذي يُشارِك في هذه التبادلات، وهل هذه العوامل يمكن الوثوق بها أم لا.

هذه الإتجاهات تشير إلى بدايات نظام جديد لحكم الهُوية، في هذه البيئة، يتحدَّى الأفرادُ والمصالح التجارية سلطة الدولة في وساطة الهُوية، ولا تزال الحكومات على الأرجح تحتفظ ببعض الصلاحيات لتحديد شروط الهوية الرسمية عن طريق التحكم في الوصول إلى بعض الامتيازات والمنافع؛ ومع ذلك، فإن الأفراد لديهم على نحو متزايد القدرة على السيطرة، والتفاوض، والتعامل مع الهويات الخاصة بهم، وخاصة في البيئة الرقمية، والمصالح التجارية تظهر وكأنها مقابل استئجار الميسرين للمساعدة على إدارة هذه الهويات الشخصية، باعتبارها خدمة عملاء صريحة أو لغرض تسليع معلومات الهُوية لاستخدامها من قِبل أطراف ثالثة.

وتعكس هذه التغييرات مفارقةَ كيفية تطوُّر الهوية في المجتمع، فمن ناحية، فهذه التكنولوجيات تمكِّن التخصيصَ أكثر من الخبرة، ويظهر هذا في التوسع في استخدام وسائل الإعلام الاجتماعية، وتفريد التعليم والطب والتكنولوجيا المراقبة الحيوية المستمرة، وتطبيقات الجوال الأمثل للعادات الفردية، التفضيلات الشخصية، وأنماط الحياة اليومية، ومن جهة أخرى، تدفع قوى مضادة لخيارات التقنية المحسنة لحماية الخصوصية والمعلومات الشخصية، وضمان عدم الكشف عن الهوية في البيئة الرقمية، ويتَّضِح ذلك في التوسع في استخدام التشفير القوي، وتزويدِ الأفراد بالقدرة على التواصل بشكل آمن وإجراء معاملاتهم الخالية من المراقبة.

قد تعكس الازدواجية العامة على القضايا الأمنية للخصوصية الشخصية، عمومًا هذا التوتر، ووفقًا إلى دراسة بيو التي أُجريتْ مؤخَّرًا، فإن نحو 93 في المائة من البالغين في الولايات المتحدة يعتبرون أنه من المهم أن يتم السيطرة على من يستطيع الحصول على المعلومات المتعلقة بهم، ومع ذلك، يشعر القليل منهم (63 في المائة) بأنه من المهم أن تكون قادرة على "التنقل في الأماكن العامة دون تحديد دائمًا"، ومع ذلك، فتشير نتائج الدراسة أيضًا إلى أن معظم الأميركيين يتوصل إلى حد ما إلى أن حقيقة الكثير من النشاط الرقمي الخاص بهم لا يظل خاصًا وآمنًا، وحتى أقل من الذين لديهم الكثير من القوة للسيطرة على كيفية استخدام هذه البيانات. وعلاوة على ذلك، فحتى تمسُّك الأمريكيين بالرغبة في عدم الكشف عن هويتهم الرقمية، يتَّخِذ عددٌ قليل جدًّا منهم الإجراءات التقنية الاستباقية لتعزيز الخصوصية أو حماية النشاط على الإنترنت من المراقبة، ومن المرجح أن تظلّ هذه المواقف المتضاربة في توتُّر، وسوف تلعب دورًا هامًّا في تشكيل مستقبل الهُوية، بما في ذلك علاقتها بالأمن القومي، ولعلّ الأهم من ذلك، سرعةُ وتيرة التغير التقني التي تعني على الأرجح أنَّ الحكومة ستكون في ردِّ الفعل بدلًا من الدور الاستباقي لتشكيل كيفية تطوُّر مفهوم الهوية في المستقبل.

التغيير الذي من المحتمل أن يكون له آثارٌ كبيرة على الأفراد وكذلك الحكومات هو فكرة دمج الهوية، فإلى اليوم، لا تزال معلومات الهُوية غير متجانسة إلى حدٍّ ما؛ من حيث شكْلها وكيفية تخزينها واستخدامها، بِناء الهوية التقليدية مثل الفسيفساء ثنائي الأبعاد، يتكون من عدد وافر بدون تداخُل، ويكون هناك تنسيقٌ واضح من المعلومات، ويمثِّل ذلك من خلال مجموعة من المصادر بما في ذلك الوثائق التي تُقرُّها الدولة (جوازات السفر وشهادات الميلاد)، معلومات حول السيرة الشخصية غير الرسمية (مقالات الصحف، وعضوية النادي)، والبيانات الحيوية المعلوماتية (السجلات الطبية، والوصفات الطبية، وثائق التأمين)، وسائل الإعلام الرقمية (سجلات الشبكات الاجتماعية والبريد الإلكتروني والهاتف)، ويحتوي هذا البناء على وجود كمية هائلة من المعلومات الخاصة بالهُوية، ومع ذلك، فإن الكثير من هذه البيانات غير مجزأةٍ للغاية وقابلة للتلف (في شكل السجلات المادية)، أو الاحتفاظ بها في صيغ تجعل من الصعب اكتشاف وجود ارتباط بين المعلومات، وتحليلها، وبالإضافة إلى ذلك، فعلامات الهوية التقليدية عمومًا مبنية على محتوى واضح؛ مثل: أسماء الأسرة، وأرقام الهاتف، وعنوان السكن، العمل، وأرقام الضمان الاجتماعي .... إلخ.

ومِن المرجَّح أن تكون مختلفة جدًّا عن النموذج القائم على خصائص بناء هُوية جديدة، وسوف يكون أقلَّ مِن الفسيفساء وأكثرَ من مركَّب متجانس الذي تم تعريفه من قِبل العلاقات المتأصِّلة المستمدَّة من الارتباطات التحليلية بدلًا من المعلومات الواضحة، ولن يتم تعريف هذه الهويات الضمنية التي سوف تخفي الفروقَ القائمة بين المعلومات البيوغرافية، البيومترية والسلوكية، والرقمية، فهذه الهويات المركبة تكون مستمرة، تراكمية، وترابطية، مما يعني أنها ستعتمد على المعلومات التي تدوم إلى الأبد في الأرشيفات الرقمية، تتراكم نقاط البيانات باستمرار كالجديدة، ويتم إثراء المحتوى من خلال ارتباط عميق بالأشخاص الآخرين، الأماكن، والأنشطة، وهذه الهويات الجديدة غير موجودة كعُقَدٍ منفصلة من البيانات، ولكن

سيتم تحديدها في سياق علاقتها بالأمور الأخرى. وهكذا، فمفهوم الهوية في المستقبل سيكون شبكة بطبيعته، ومتعدد الأبعاد في الطرق التي لن تكون بها الهويات الحالية.

هناك تلميح لهذا المستقبل الواضح بالفعل في كيفية استخدام الأفراد لتقنيات الهواتف الذكية والأجهزة الأخرى المتَّصِلة بالشبكة، ويتم تمكين العديد من تلك التقنيات بالفعل مع مصادقة الوسائط البيومترية المتعددة (بصمات الأصابع، القزحية، الوجه، والتعرف على الإيماءات)، وهذا يعني أن أيَّ نشاط يرتبط مع جهاز معين يمكن أن يكون مرتبطًا مع توقُّعات الهوية الفريدة الأخرى؛ مثل: الصوت وبيانات الإرسال، والأنماط السلوكية، والحركات الفضائية، ونشاط الشبكة الاجتماعية.

وسيكون أحد الآثار المترتبة على هذا الاندماج هو الهوية، وسيكون احتمال وسائل أكثر قوة من المراقبة السلبية، كما يتم دمج الهويات الرقمية على نحو متزايد مع غيرها من البيانات البيومترية والأنماط السلوكية، ومعلومات حول السيرة السياقية، قد يصبح من السهل أيضًا كشف أعمال الخداع المتعمدة، وكيل وزارة الدفاع لشؤون الاستخبارات مايك فيكرز لاحظ في الآونة الأخيرة كيف أصبح من السهل تتبُّع الأفراد في جميع أنحاء العالم في السنوات الأخيرة بسبب "الغبار الرقمي الذي نتركه جميعًا ونحن نمضى في حياتنا."

ويدل جوجل بالفعل على بعض الأمثلة العملية لمفهوم تغيير الهوية مع النظام الأمني في الوقت الحقيقي، باستخدام مزيج من التعرف على الوجه، والكشف عن الصوت والبيانات السلوكية لتمكين مصادقة الجهاز بشكل مستمر دون استخدام كلمات المرور التقليدية، ومن المرجَّح أن التركيز على هذه التوقيعات غير التقليدية وأجهزة الاستشعار قادرة على كشف وتسوية مجموعة واسعة من المعرفات المنفصلة والغامضة للمرحلة المقبِلة من الحرب الإلكترونية، هذا وسوف تكون جنبًا إلى جنب مع الأدوات التحليلية الجديدة قادرة على اكتشاف وربْط هذه السمات من البيانات والجداول الهائلة من المعلومات

غير المتجانسة والمجزأة، والقسم الأخير من هذه الدراسة يَدرُس العديدَ من مناطق التكنولوجيا الناشئة، ومناقشة إمكانية تطبيق هذه الأدوات، والنظر في الكيفية التي قد تشكِّل كيفية شن الحرب الإلكترونية في المستقبل.



مستقبل التقنية: شن الحرب الإلكترونية في الأجيال القادمة

تتناول مناقشة السيناريو والتكنولوجيا الثلاثة التالية المهام المترابطة التي تعتبر أساسية للحرب الإلكترونية: اكتشاف الهوية، نسب التفعيل، ورسم خرائط الشبكة، وفي أثناء وصف هذه المهام، يستكشف هذا القسم عددًا من مجالات التكنولوجيا الناشئة فقط وراء الأفق التشغيلية، بينما يقصِد أن نكون واقعيين، وتجدُر الإشارة إلى أن هذا السيناريو يَفترِض بعض القدرات التنظيمية والأساليب التشغيلية، وسياسات تقاسُم المعلومات التي لم تكن موجودة، ومع ذلك، تقدم الدراسة حالة افتراضية لسياق دراسة كيفية تطبيق مجموعة من الأدوات التقنية الجديدة قريبًا، لاستخدامها في العمليات، وكيفية شن الحرب الإلكترونية في المستقبل.

المهمة الأولى: تحديد الهوية

دخل شاب يتحدث الإنجليزية بلكنة غير مرتبة إلى مطار أتاتورك باسطنبول مع تذكرة ذهاب فقط إلى أمستردام، وحذائه مغطاة بالطين، وقميصه قديم قليلًا، ويوحي مظهره بأنه ظل عدة أيام دون استحمام، كما أنه يدخل في مجال مراقبة الهجرة، ويبدو أنه خائف بشكل واضح، كما أنه اقترب من المخلص الجمركي. وقال: إنه لم يمرَّ على فحص الأمتعة، ولديه فقط حقيبة ترحال صغيرة تحتوي على الهاتف الخليوي، ومحرك أقراص USB، وثائق السفر، وعدد قليل من البنود الشخصية، أَمَر الوكيل بفحص بطاقته الداخلية، وإظهار معلومات سجل أسماء الركاب على الشاشة لإعطاء اسمه وعنوانه ورقم بطاقة الائتمان المرتبطة بشراء التذاكر، ولاحظ الوكيل رسالة تنبيه تشير إلى أن رقم جواز السفر قد أُدرِج مؤخرًا في قاعدة البيانات المسروقة ووثيقة السفر المفقودة من الإنتربول، من خلال الفحص الدقيق، لاحظ الوكيل أن الصورة تبدو مختلفة بعض الشيء في جواز السفر عن مظهر الرجل، وبناء على تلك المخاوف، تم سحب المشتبه به جانبًا لفحص ثانوي، و تقرَّر أنَّه غير مسموح به على متن الرحلة.

التحدي الأول من هذا السيناريو هو حل هُويَّة شخص مشبوه يحمل جواز السفر تحت وثائق مزورة، هناك عدة أساليب للقياس الحيوي القياسي قيد الاستخدام حاليًّا لتأسيس الهوية وفحص الأفراد من معلومات قائمة المراقبة. وتشمل هذه الطرائق البيولوجية الأكثر شيوعًا من الوجه، وبصمات الأصابع، وقزحية العين، في حين لا يزال التعرف على الوجه إلى حدٍّ ما أقل موثوقية من الأساليب البيولوجية الأخرى للتحقق من الهُوية؛ حيث له مزايا أكثر من الأساليب الأخرى التي عادة ما تتطلَّب التعاون

والاتصال المباشر، من ضِمن الأساليب القياسية، قد شهد التعرف على الوجه ربما أعظم تغيير في السنوات الأخيرة، ويرجع ذلك جزئيًّا إلى مجموعة متنامية من التطبيقات التجارية.

ذكَر تقييم الأداء الأخير من خوارزميات التعرف على الوجه الذي أجراه المعهد الوطني للمعايير والتكنولوجيا؛ أنَّ الدقة الشاملة في المجال قد تحسَّنت ووصلت إلى 30 في المئة منذ عام 2010، فعلى سبيل المثال، قد تحسَّنت خوارزميات تعزيز التطبيقات للكشف عن جواز السفر، وتطبيقات رخصة القيادة الاحتيالية، طرق لمراقبة الدخول ومراقبة المنطقة، والطب الشرعي الرقمي في التحقيقات الجنائية.

ومن بين التطبيقات التجارية، هي الفيسبوك التي تراكمتْ لديه تقديرات الخبراء في أن تكون أكبرَ قاعدة بيانات للتعرف على الوجه في الوجود، وتُستخدَم لتحديد ووضْع علامات الأفراد التي تظهر في الصور، وفْقًا لفريق الأبحاث، فقد حقَّق برنامج مطابقة الوجه دقة حوالى 97 في المئة لمطابقة الوجوه بين صورتين غير مألوفتين، ومستويات الأداء تعادِل تقريبًا قدرة الإنسان، وهذا يشمل الصور التي تم التقاطها تحت ظروف الإضاءة المتغيرة، وحتى في بعض الحالات التي لا تُوجَّه مباشرة إلى الكاميرا.

تَطبيقاتُ العمل التقليدية للتعرف على الوجه بشكل عام من خلال تطبيق الخوارزميات لاستخراج ملامح من الصور باستخدام واحدة من الطريقتين. الأول هو الهندسي، أو الروائي الذي يعتمد على تحليل بِنية الوجه إلى مكونات تُعرف باسم (eigenface). ثم تتمُّ مقارنةُ هذه المكوَّنات مع صور أخرى عن طريق قياس المسافة بين سمات كل منها، النهج الثاني، يشير إلى الضوئية، أو عرض القائمة، ويستخدم المنهج الإحصائي لاستخلاص صورة في القيم ومقارنتها مع نماذج معروفة، مع أي من الطريقتين، تشمل التحديات التقنية الكبرى التي تتعامل مع الصور ذات الجودة المنخفضة، والتغيرات في المظهر، وتشكيل الاختلافات، بالإضافة إلى ذلك، هناك عدد من القيود التقنية من حيث التقاط الصور

القابلة للاستخدام في المسافات الطويلة، أثناء الليل، ومن الصور منخفضة الدقة من النوع التي تم الحصول عليها من كاميرات الويب وكاميرات أجهزة الصراف الآلي، أو فيديو للمراقبة.

وقد ظهر تحديدُ الوجه على أساس مزيج من البيانات وصور الأشعة تحت الحمراء D3 كطريقة واحدة مُحتمَلة لتعزيز النهج الحالي، ويمكن تحقيق ذلك عن طريق تحويل الصور2 D إلى D3، وذلك باستخدام النمذجة الرياضية من أجل التقاط البيانات المفقودة في الصور القياسية، بالإضافة إلى ذلك، فإن صورَ المسح الضوئي ثلاثية الأبعاد جنبًا إلى جنب مع النمذجة الحرارية توفِّر وسيلة للتغلب على التحديات مع اختلاف التخفي وظروف الإضاءة التي يمكن أن تُقلِّل من الدقة، وهذه الأساليب هي أيضًا من الناحية الفنية أكثر صعوبة في محاكاة النهج القياسي الساخرة.

تقنيات المسح ثلاثية الأبعاد الحالية هي أكثر مُلاءمة للوصول إلى التحكم بدلًا من المراقبة، ومع ذلك، قد تُقدم التطورات الأخرى قريبًا توسعًا للأساليب. يشمل استخدامَ تحليل الململس، وتحسين خوارزميات استخراج الصور من فيديو الأشعة تحت الحمراء، فضلًا عن أساليب استخدام الصور المركبة المشتقة من أشرطة الفيديو المتعددة، وتشمل المناهج الأخرى استخدام طوبولوجيا ثلاثية الأبعاد والكاميرات القادرة على التقاط البيانات خارج الطيف المرئي؛ مثل: الأشعة تحت الحمراء القريبة وموجة الأشعة تحت الحمراء الحرارية، ويمكن أيضًا أن تُستخدَم مِثلُ هذه الأساليب لجمع التوقيعات الفسيولوجية، بما في ذلك درجة الحرارة والنبض وضغط الدم.

ما وراء تقنيات التصوير، من المرجّح أن يأتي من مِزيج من زيادة قوة المعالجة والتحسينات في استخدام مكاسب الذكاء الاصطناعي (AI) الرئيسة التالية في التعرف على الوجه، وتشير منظمةُ العفو الدولية عمومًا إلى فَرْعي علوم الحاسوب للتعامل مع الخوارزميات، التي تركِّز على المهام التي تتطلَّب عادة التحليل البشري؛ مثل: الإدراك البصري، والتعرف على الكلام، وحل المشكلة المجردة، وكثيرا ما ترتبط منظمة

العفو الدولية مع مفهوم "البيانات الكبيرة" حيث يُرجَع ذلك إلى حقيقة أن هذه المجموعات الكبيرة عمومًا يجب تحليلها من خلال الأساليب الحسابية، فخوارزميات منظمة العفو الدولية عمومًا مفيدة جدًّا لتحليل وتفسير هذه البيانات؛ للكشف عن الأنماط والإتجاهات والروابط كجزء لا يتجزَّأ في مجال الذكاء الاصطناعي، وهو منطقة متميِّزة تُسمَّى التعلمَ الآلي؛ حيث ينطوي على استخدام خوارزميات متخصِّصة قادرة على "التعلم" من البيانات نفسها وتقديم النماذج التنبؤية من خلال تحليل الأنماط، فئة واحدة من التعلم الآلي المعروف باسم "التعلم العميق" تَستخدِم الصيغ الرياضية لتكرار "الشبكات العصبية" من خلال محاكاة العمليات التحليلية في الدماغ البشري، وقد أثبتت هذه الأساليب إمكانية كبيرة لتحسين دقة وقوة أساليب القياس الحيوي القائمة، ولا سيما في مجالات اللغة، والتعرف على صور الوجه.

وقد وجدت في مفهوم الشبكات العصبية لعدَّة عُقود، ومع ذلك، كانت التطبيقات العملية محدودة القدرة الحاسوبية، وتضمن عدم وجود قواعد بيانات كبيرة بما فيه الكفاية لتحسين "التدريب"، ويحدث هذا التدريب عن طريق تَكرار عملية "تعلم" الكمبيوتر لكيفية التعرف على السمات بشكل متزايد أكثر تعقيدًا، مِثل:

مجموعات الصور أو الملفات الصوتية، على سبيل المثال، واحدة من التحديات الفنية الأكثر شهرة في مجال التعرف على الصور تنطوي على مهمة الإنسان البسيطة نسبيًّا في تعلم الكمبيوتر لتحديد صور القطط بين مجموعة من الصور غير ذات صِلة، أظهر باحثون جوجل مؤخرًا تحسنًا كبيرًا في هذه المهمة، وذلك باستخدام أساليب التعلم العميق لفرز وتحديد صور الهدف من نحو 10 ملايين من الأمثلة الواردة في أشرطة فيديو اليوتيوب، وقد استُخدِمت أساليب مماثلة لزيادة سرعة ودقة التطبيقات التجارية والتعرف على الصور؛ مثل: تلك المستخدَمة من قِبل الفيسبوك، وجوجل، ومايكروسوفت، وتويتر.

هذا ومِن المرجَّح أن تُقدِّم تطبيقُ أَساليب التعلم العميق والشبكات العصبية تحسيناتٍ كبيرةً لصور وفيديو تحليلات الأداء، ويحتمل أن تُتيح البحثَ السريع ومطابقة الكميات الهائلة من ملفَّات الوسائط، وتمثِّل هذه المهمة واحدةً من العقبات التقنية الرئيسة في عهد "البيانات الكبيرة"، على سبيل المثال، من المتوقَّع أن تتضمَّن نحو 52 مليون صورة وجه بحلول عام 2015 في قاعدة بيانات مكتب التحقيقات الفدرالي البيومتري، في حين أنَّ وزارة الخارجية الأميركية لديها بالفعل عقدٌ أكبر من الصور لطالبي التأشيرات، فالفرز من خلال هذه الملفَّات يمثِّل مهمةً محددة نسبيًّا للمطابقة داخل نظام مُغلق يحتوي على بيانات موحَّدة وضوابط صارمة على جودة الصورة، ومع ذلك، لا تَنْطوي على التحدي التقني الأكبر بكثير في استغلال المعلومات من قواعد البيانات غير المهيكلة؛ مثل:

فَرْز كميات هائلة من محتوى الوسائط الاجتماعية بحثًا عن الارتباطات ذات المغزى، وهذا ينطبِق بشكل خاص على مجموعات المحتويات الغامضة، والمحتويات غير المنسقة أو الملفات مع البيانات الوصفية المرتبطة بذلك، وقد تنطوي التحديات الأخرى على مطابَقة البيانات غير المتجانسة؛ مثل: مهمة مقارنة الصور التي تم الحصول عليها من الضوء المرئي مُقابل أنظمة الأشعة تحت الحمراء القريبة.

وقد أظهرتِ العديدُ من النماذج الأولية الأخيرة كيف تساعد الشبكات العصبية على التغلب على بعض هذه القيود مثل القدرة على التعرف على صور الوجه من الزاوية أو عندما يُغطي جزئيًّا. وقد طبَّق الباحثون هذه الأساليب لتحسين خوارزميات الكشف الآلي لملفات الفيديو، ونقل التكنولوجيا لخطوة أقرب إلى وجود القدرة على التحليل في الوقت الحقيقي من الفيديو الرقمي أو كاميرات المراقبة "الدوائر التلفزيونية المغلقة" (CCTV).

قد يكون المعيار الذهبي في المستقبل من أجل التعرف على الوجه هو القدرة على الجمع بدون روابط، في حدود المعقول، بين الأفراد المتعددون، مع تحديد الوقت الحقيقي، بعض التقنيات المتوفرة حاليًّا تدلُّ على أن الإتجاه قد يتحرَّك إلى هذه القدرة، على سبيل المثال، المنتج التجاري الجديد قادرًا على التقاط صور الوجه من لقطات فيديو حيَّة، ثم ترجمتها على الفورِ إلى أي محتوى ذات صِلة بالهُوية من مواقع وسائل الإعلام الاجتماعية والمصادر المفتوحة الأخرى لإنشاء ملف تعريف للشخص في الوقت الحقيقي.

وكانت هناك أيضًا تحسينات أخيرة في التقنيات الحالية لتعزيز سرعة ومرونة الالتحاق البيومتري، مثل جمع صور القزحية في ثوان معدودة والقدرة على التقاط البصمة، الكاميرات عالية الدقة الآن تنتج صورًا عالية الجودة للتعرف من مسافة عدة أمتار تحت ظروف معينة، مع بعض النماذج حتى توسَّع نطاقُ هذا التأثير إلى أنْ تراوح من 100 - 200 متر، وقد ظهر احتمال استخدام هذه القدرة مؤخرًا من قِبل مجموعة ادَّعت حصولَها على بصمات الأصابع، القابلة للاستخدام لوزير الدفاع الألماني المستمدَّة فقط من صورة رقمية، والتي اتُّخِذت على مسافة، خلال الاشتباك، قيل: إنَّ الصورة تم الحصول عليها باستخدام كاميرا رقمية متوفرة تِجاريًّا، وتم المسح خوارزميًّا للبصمة المشتركة.

الأساليب المختلفة خاضعة للتنمية من أجل التعرف على بصمات الأصابع بدون اتصال بالأجهزة الرقمية المحمولة وغيرها، وتم إحراز تقدُّم مماثل في التقاط البيانات القزحية الصالحة للاستعمال تحت ظروف أشعة الشمس التي تُعدُّ العامل المحدّد الرئيس لهذه الطريقة، وقد أثبتت شركة أخرى أن نموذج المسح القزحي قادرٌ على جمع الصور، التي يمكن استخدامها في أكثر من 30 ياردة ضد هدف ثابت، مع ذلك، لا تزال هذه التكنولوجيات جاهزة بعد سنوات للاستخدام العملي، الجهود الأخرى على استكشاف الاختلافات حول الأساليب الأساسية؛ مثل: استخدام أنماط الأوعية الدموية في العين، خلافًا لقزحية العين ومَسْح شبكية العين، يمكن الحصول عليها مع الكاميرات الرقمية القياسية بدلًا من بواعث الأشعة تحت الحمراء.

بين الأساليب القياسية، هناك هدف آخَر مهمٌّ يَنطوي على أساليب محسَّنة لتكامل البيانات متعددة الوسائط، وبذلك على وجه التحديد قزحية العين، البصمة، وتصوير الوجه إلى "نمط الحياة" مركب الشخصية من الموضوعات الفردية، الأبعد من هذه التقنيات، عدد غير تقليدي من أساليب القياس الحيوي، التي تتَّجه تدريجيًّا نحو الاستخدام العملي، بما في ذلك نمط الأوعية الدموية، وهيكل الأذن، هندسة اليد، المشية، والرائحة، وطباعة النخيل، وتخطيط القلب، والطريقة غير التقليدية الأخرى الآن التي تُستخدَم على نطاق واسع هي تحديد الندوب والعلامات، والوشم، وتحدَّد قاعدة البيانات التالية في مكتب التحقيقات الفدرالي مؤخرًا القدرة المتكاملة، وتعرض مطابقة كل صورة والاستفسارات على أساس الكلمات الرئيسة الوصفية، في حين لم تحدَّد بشكل فريد في العُزلة، وتوفِّر هذه الأدواتُ وسيلةً أخرى للتحقُّق من الوسائط المتعددة التي يحتمل أن تحسِّن مِن الدقة عندما ترتبِط مع غيرها من الصفات؛ مثل: الحمض النووي وبيانات السيرة الشخصية، والأنماط السلوكية، والرقمية وتوقُّعات وسائل الإعلام.

وكانت هناك طريقة أخرى مع المكاسب التي تحقَّقت مؤخَّرًا في الاعتراف بأداء مجال اللغة؛ كالبيومترية، أنظمة التعرف على المتحدِّث الآلي يُمكن "استخراجُ، تمييزٍ، والتعرف على المعلومات في إشارة خطاب نَقْل هُويَّة المتكلم"، وبصفة عامَّة يمكن القيام بذلك مع مجرَّد عيِّنة صوت قصيرة؛ حيث توفِّر بيانات كافية لقياس الصفات الصوتية الفريدة للفرد وإنتاجه، هناك العديد من الجهود الحالية في مجال مصادقة الهُوية والكشف عن الغشِّ، ويتم استخدامها في الخدمات المصرفية، وعمليات مركز الاتصال، واجهة الجهاز الرقمي، وقد أدَّى ذلك إلى التوسع السريع في عدد الأفراد الذين يستخدمون هذه التقنية مع دراسة بحثية لتقدير ذلك، بحلول عام 2019، فإن هناك خمسة مليار شخص قد خُلِقوا ببصمة صوت شخصية، ويتكهَّن الخبراء أنه يمكن أن تحتوي على نحو 65 مليون بصمة صوت فريدة بالفعل في مجال إنفاذ القانون في الولايات المتحدة وقواعد البيانات على أجهزة الاستخبارات؛ وذلك للتوسع بشكل كبير في السنوات المقبلة.

ويُقدِّم الصوت البيومتري العديدَ من المزايا الواضحة على الأساليب الأخرى. وقد وصِف البيومتري بأنَّه "غير مرئي"؛ لأنه لا يتطلَّب اتصال مباشر للجمع، كما يمكن الحصول على بصمة صوت من مجموعة من أجهزة الاستشعار (ميكروفون، والهواتف، وأجهزة الكمبيوتر، وغيرها)، ومع ذلك، فهناك العديد من القيود المفروضة على التكنولوجيا الحالية، بما في ذلك صعوبة المقارنات بين الهاتف الثابت والتسجيلات الخلوية، أو الميكروفون، فضلًا عن قضايا التعامل مع الضوضاء المحيطة، والاختلافات اللغوية، أو المعالجة الحكمية غير العادية؛ مثل: الهمس، وينطوي التحدي التقني الرئيس الآخر على التعامل مع تداخل الكلام من مكبِّرات الصوت المتعددة على عينة صوتية واحدة.

حين يتم جَمْع البيانات الصوتية، يتم عمومًا تطبيق النهج التقليدي من النماذج الإحصائية لتمثيل الاختلافات في الأشكال السليمة، أو الفونيمات، الفريدة من نوعها لصوت الفرد، نماذج ماركوف المخفية (HMM) كانت تقنية إحصائية مهيمنة لإدراك المتحدِّث الذي يعتمِد على النصِّ (عندما يكون هناك معرفة مُسبَقة بالنصِّ قبل التحدث)، وغالبًا ما تُستخدَم طريقة ذات الصِلة، والمعروفة باسم نماذج خليط غاوسي، على النص المستقل، أو الخطاب المرتجل، حيث لا تتطلَّب التعاونَ مِن قِبل المتحدِّث، في كلتا الحالتين، يتم مقارنة أنماط الصوت الرقمية لتخزين بصمة الصوت من أجل إنتاج قرار الإدراك، وتطبَّق النماذج الإحصائية المماثلة لمهام التعرف على الأنماط الأخرى؛ مِثل: معالجة اللغة الطبيعية على خط اليد، وطريقة HMM وراء نموذج VIBES الحالي للجيش يتم استخدامها لتحديد وتتبُّع الأفراد وتحليل شبكات الاتصالات التكتيكية.

كما هو الحال مع تقنية التعرف على الوجه؛ حيث أدَّت التطورات الحديثة في التعلم الآلي وزيادة قوة المعالجة إلى تحسينات كبيرة في الأداء، ويتمُّ حاليًّا استخدام الشبكات العصبية على قواعد بيانات كبيرة من الملفات الصوتية لتحديد المجموعات تدريجيًّا الأكثر تعقيدًا من الفونيمات، وهذا يُتيح للبرامج "التعلمَ" مع مرور الوقت، دون تدخُّل بشريٍّ والتعامل بشكل أفضل مع الغموض في النحو، وكذلك

الاختلافات في استخدام اللهجة، وتوفِّر أساليب التعلم العميقة والشبكات العصبية أيضًا نَهجَ تعزيز إشارة البيانات ذات الجودة المنخفضة، من خلال تصفية الأصوات غير مرغوب فيها، وإزالة الضجيج، وحتى إزالة غموض تعدُّد الأصوات على قناة واحدة، ويمكن أيضًا التغلب على بعض الصعوبات التقنية التي تُصادَف مع عدم تطابُق نوع الصوت، مشاريع البحوث المتقدمة لوكالة الدفاع (DARPA) تستكشف حلول لبعض من هذه القضايا من خلال النسخ التلقائي القوي لبرنامج الكلام، الذي يهدُف إلى فَصل الخطاب عن الضوضاء في الخلفية، وكذلك المهام ذات الصِّلة؛ مثل: تحديد اللغات التي يتحدَّث بها من الملفِّ الصوتي، وعَزْل الكلمات الرئيسة ضِمن تلك العينة.

ويُجرِّب الباحثون أيضًا التطبيقات الجديدة المستمدَّة من بيانات البصمة الصوتية؛ مثل: تحديد الحالة العاطفية للفرد، ويتضمَّن أحدُ الأمثلة على الفحص الطبي الحيوي للاضطرابات العصبية، باستخدام مزيجٍ من العلامات المستمدة من وظائف التحكم في المحركات مرتبطة الرأي والتعبير في الوجه، وقد قام فريق من معهد ماساتشوستس للتكنولوجيا بمختبر لينكولن(MIT) مؤخرًا بإظهار تطبيق باستخدام المؤشرات الحيوية والصوتية للوجه كأداة تنبؤية لتحليل الحالة المعرفية للفرد، وتقوم وزارة الأمن الداخلي باستكشاف القدرات ذات الصِّلة لاستخدامها في فَحْص نقاط التفتيش، على سبيل المثال، باستخدام مجموعة من حركات الوجه، والعيِّنات الصوتية، وأجهزة الاستشعار الفسيولوجية للكشف عن أمراض الجهاز التنفسي، وأمراض القلب، والحرارية، وقزحية العين وردِّ الفعل كوسيلة لتحديد النية العدائية أو السلوك المشبوه بين الحشود.

ويتكهَّن بعض الباحثين أنَّ هذه الأساليب قد تمكِّن قريبًا أجهزةَ الكمبيوتر من تجاوُز البشر في القدرة على إدراك العواطف الأساسية، وقد أثبتتْ (DARPA) فائدة الأدوات الآلية لتحديد الضيق النفسي، والاكتئاب، والقلق، وكانت هناك أيضًا أمثلةٌ ناجحة لتطبيق برنامج التعرف على الوجه لرمز التعبيرات العاطفية، على أساس حركات متميزة من عضلات الوجه والعينين والخدين والشفتين، وغيرها

من الصفات، ويحقق النموذج التجاري مؤخرًا معدَّل الدقة بناء على 97 في المئة في تحديد العواطف الستِّ الأساسية، و77 في المئة لبعض العواطف المجمَّعة.

وما وراء الأساليب القياسية، المتزايدة في مجال القياسات الحيوية السلوكية يُحتمل أن تقدِّم مجموعة من الطرق الجديدة لإقامة الهوية عن طريق وسائل غير مباشرة، بصفة عامة، تشير القياسات الحيوية السلوكية إلى الخصائص التي يتم تعلُّمها أو اكتسابها بمرور الوقت بدلًا من تلك التي تَستنِد في المقام الأول على علم الأحياء، على سبيل المثال، تشمل هذه المهارات، الأسلوبَ، التفضيلَ، والمعرفةَ، والمهارات الحركية التي يستخدمها الأشخاص لإنجاز المهام اليومية. وبعض الأمثلة الشائعة في الاستخدام الحالي تنطوي على خط اليد، الضغطة، والديناميات، أو تحليل المشي، من الأمثلة الأخرى على تحديد الأنماط السلوكية المميَّزة المستمدَّة مِن الأنشطة؛ مثل: روتين البريد الإلكتروني، وتفاعلات الجهاز، واستخدام بطاقة الائتمان.

القياسات الحيوية السلوكية لديها عدد من المزايا على القياسات الحيوية التقليدية، وأبرزها إمكانية جَمْع البعيد أو غير المتوافق، على الرَّغم مِن أن القياسات الحيوية السلوكية غالبًا ما تكون أقلَّ دقَّة من المقاييس البيولوجية، ويمكن استخدامها جنبًا إلى جنب مع الأساليب الأخرى أو تطبيقها بشكل غير مباشر؛ لتحديد خصائص الأفراد ضِمن عددٍ أكبر من السكان، على سبيل المثال، يمكن أن يشمل ذلك تحديدَ مجموعة من الأشخاص الذين يعانون من سِمة مميَّزة؛ مثل: معرفة الكلمة، الكفاءة الرياضية، أو مهارة في مهمة محددة مِثل: التحدث بلغة أجنبية، في حين لم تُحدّد بشكل فريد في العزلة، يمكن أن تكون هذه المعلومات السياقية مفيدة في تحليل الشبكات عن طريق تصنيف وظائف الأفراد أو عقد الشبكة.

أنماط النشاط الأخرى مِثل استخدام البريد الإلكتروني أو تصفُّح الإنترنت توفِّر إمكانيةَ استخلاص تعريف المِستخدم الفريد من نوعه مع الاستفادة من مجموعة غير نافرة، قد أظهرت دراساتٌ متعددة كيف يمكن أن تستمدَّ الملامح السلوكية الفريدة من خصوصيات استخدام البريد الإلكتروني، بما في ذلك أسلوب الرسالة، والنشاط الزمني، والهيكل، وغيرها من المتغيرات، وهذا له تطبيقات واضحة لحسم الهُوية الغامضة المستمدة من حسابات المستخدم المشتركة من قِبل الأفراد المتعددين أو الوصول إلى أجهزة الكمبيوتر العامة، وقد تم تطوير تطبيقات مماثلة لرصد السلوك المنحرِف على منصات وسائل الإعلام الاجتماعية، والكشف عن حسابات تويتر والفيسبوك الوهمية، ويمكن أن يساعد تحليلُ الأنماط السلوكية في تأكيد صحة مصدر الفاعلين المجهولين على وسائل الإعلام الاجتماعية أو الكشف عن أوجه التشابه بين نمط العديد من المستخدمين عبر المنصات، ويمكن أيضًا أن تُطبَّق القياسات الحيوية السلوكية للمساعدة في تحديد حملات التضليل على الإنترنت عن طريق تحليل الإشارات اللغوية، وأنماط الاستخدام والصلات الاجتماعية، والمواقع المادية لتصنيف الهويات وراء الوظائف، فعلى سبيل المثال، استُخدِمت الأساليب المماثلة مؤخرًا لتحليل الوظائف الشاغرة للعسكريين الروس من أجل تجهيزهم للعمليات في أوكرانيا.

مثال آخر على البيومترية السلوكية الأكثر شيوعًا هو استخدام أنماط بطاقة الائتمان؛ لحماية الاحتيال من قِبل القطاع المصرفي، وتنطبِق تقنية تلك الأساليب الإحصائية لتحديد السلوكيات الشاذة؛ مثل: المعاملات غير العادية، والمواقع الجغرافية الجديدة، أو استخدام البطاقة في وقت واحد في مواقع متعددة، وحسَّن هذا المجال وسيلةَ تحليل أكثر من 400 صفة سلوكية حيوية ومعرفية، وصفات فسيولوجية لإنشاء ملفات تعريف المستخدمين الفردية العالية، وقد أصبحت هذه التقنيات شائعة في أمْن البنوك وغيرها من التطبيقات؛ حيث يمكن استخدام التعريف المجهول لتحليل السمات السلوكية الفريدة للفرد، وعَرَض فريق من مختبر معهد ماساتشوستس لتكنولوجيا وسائل الإعلام هذه القدرة عندما حدَّد نحو 90 في المئة من

الأفراد من مجموعة العينة، التي تَستنِد فقط على مواعيد وأماكن مجموعة من معاملات بطاقات الائتمان جنبًا إلى جنب مع وسائل الإعلام الاجتماعية، وقد تحقَّق ذلك من دون معرفة مُسبَقة للأسماء، العناوين، أو غيرها من المعلومات المتعلِّقة بحامل البطاقة.

تقوم القياسات الحيوية السلوكية على تحديث أيضًا نهج الأساليب التقليدية مثل تحليل الكتابة، وهي تقنية وثيقة تستخدم لسنوات عديدة كأداة تحديد في الطب الشرعي، ومع ذلك، ففي العصر الرقمي، هناك عدد أقل من الوثائق المكتوبة المتاحة للتحليل؛ لذلك قد تَطوَّرت أساليب تحليل "خط اليد الرقمية" أو التواقيع الديناميكية على أساس طريقة فريدة من نوعها لأنواع المستخدم، ومعالجة الأجهزة الرقمية، ويتم حاليًّا تطبيق هذه التقنيات لمصادقة هُوية مع الأجهزة المحمولة باستخدام السمات المعرفية البيومترية التي تَعتمِد على عوامل مثل الطغيان، ورعاش الجبهة، والتنسيق بين العين واليد، وغيرها من الأنماط المحدَّدة التي تعتبر جزءًا لا يتجزَّأ من ضِمن التفاعلات بين الإنسان والآلة. قد وجدت الأبحاث هذه الأنماط السلوكية لتكون "معقدة، دقيقة، وغريزية"؛ لذلك تعتبر وسيلة دقيقة للغاية لتحديد الأفراد، بعض الأمثلة التجارية الأخيرة لمصادقة التوقيع الديناميكي المتقدم يمكن أن تَتْبَع سِمات الشخصية الفريدة عبر أربعة أبعاد، بما في ذلك الضغط، السرعة، وشكل السكتات الدماغية الساكنة، فضلًا عن السرعة والتسارع.

وقد طبَّق المتخصصون في المجال أيضًا تقنيات التعلم العميق لتحليل التعبير بلغة الجسد (الإيماءة) والتحكم في الحركة لتمكين الاعتراف بنشاط فريد من نوعه. وتشير بعض الأبحاث إلى أن هذه الأنماط الحركية هي مجرد تحديد مِثل بصمات الأصابع، فعلى سبيل المثال، استَخدَمت تجرِبة حديثة فريدة من نوعها "فيديو القياسات الحيوية المتمركزة" المستمدَّة من لقطات الفيديو الخام المأخوذة من الكاميرات المثبتة على الجسم والرأس، في هذه الحالة، تم الحصول على العلامات الحيوية الفريدة في أقل من أربع ثوان من اللقطات، عن طريق تتبُّع "التدفق البصري" من خلال إطار الفيديو، ويمكن للمرء تطبيق القدرة على

العثور على جميع مقاطع الفيديو من قِبل مستخدم واحد، من ضِمن قاعدة البيانات الكبيرة من الملفات الرقمية، حتى من دون البيانات الوصفية، واستخدمت المظاهرة الأخرى مؤخرًا لتطبيق أساليب التعلم العميق لتحسين أداء أجهزة الاستشعار المدمج في الأجهزة النقالة (الكاميرات، والميكروفونات)؛ من أجل تصنيف ما إذا كان المستخدم عليه أداء أنواع معيَّنة من الأنشطة.

وقد تمَّ تَطويرُ تقنيات مشابِهة للمصادقة البيومترية لأجهزة التلاعب بالكمبيوتر وتتبُّع اللياقة البدنية، ويتم حاليًّا استخدام معظم هذه التطبيقات البيومترية السلوكية لتحسين الأمن، ومع ذلك، فإنه يحتمل أن توفِّر وسيلة لتحديد الهوية عن بُعد، هذا يمكن أن يكون معلومات لا تُقدَّر بثمن عندما تقترن بتحديد الموقع الجغرافي الدقيق من الجهاز المحمول أو الارتباط مع نشاط وسائل الإعلام الاجتماعية الأخرى، كبشر فقد يتم الحفاظ على التفاعل شِبه المستمر مع الأجهزة الرقمية بشكل متزايد، ويقدِّم مجال المقاييس الحيوية السلوكية تقنيات مناسبة تمامًا لاستخلاص معلومات الهوية من هذه الأنشطة.

مجال آخر من طرق القياس الحيوي الناشئة هو "القياسات الحيوية المرنة"، توجد تلك الخصائص مع تحديد الصفات، ولكنها تفتقر إلى تميز واستمرارية التمييز الإيجابي بين أي شخصين، أمثلة تلك الصفات هي المساواة بين الجنسين، لون الشعر، الطول، الوزن، ونسب الجسم، لون العين، أو العرق، وتتضمَّن الفئة الأخرى من القياسات الحيوية المرنة خصائص على أساس النشاط؛ مثل: المهارات المكتسبة الفريدة أو المعرفة المتخصصة، على الرغم من أنها أقل من تحديد الأساليب القياسية، يمكن للقياسات الحيوية المرنة تقديم بعض المزايا البيولوجية والصفات السلوكية كأداة للفحص والتحليل.

أولًا: إن الكثير من البيانات، التي يمكن الحصول عليها تتمُّ بدون تطفُّل أو تكون مُشتقَّة من لقطات الفيديو ذات الجودة المنخفضة؛ حيث يكون ذلك مفيدًا لتطبيقات المراقبة الإنتاجية العالية، ثانيًّا، على عكس التوقيعات التقنية، يمكن التعبير عن القياسات الحيوية المرنة بشكل أكثر سهولة في اللغة الطبيعية،

مما يصبح من الأسهل التصنيف على أساس الأوصاف اللفظية من الخصائص الفيزيائية. وتتعلَّق هذه القضية إلى ما يسمى بـ "الفجوة الدلالية" أو الفرق بين كيفية تعبير البشر لفظيًّا عن الصفات الجسدية المتميزة مقابل كيفية تمثيلها على أنها توقيعات بيومترية.

المشكلة الرئيسة في "الفجوة الدلالية" هي أن الأوصاف الجسدية من تقارير شهود العيان ليست سهلة الترجمة إلى لغة الآلة لمساعدة الحاسوب على البحث والتحليل، وبعض الأساليب الجديدة في هذا المجال تنطوي على تحسن ترجمة الوصف الدلالي إلى التصنيفات التي يمكن استخدامها للبحث الآلي عن الصور وفيديو المراقبة، وهذا النوع من العلامات الدلالية من المحتمل أن يوفِّر تعزيزًا قويًّا للفحص بمساعدة الحاسوب، هذا قد يؤدي إلى تحسين الخوارزميات لمطابقة رسومات شاهد العيان مع الصور الرقمية، وقد أثبت باحثون آخرون كيفية وصف السِّمة العامة مِثل أنواع الملابس، ولون الشعر، ويمكن استخدامها بين الجنسين كمعايير للبحث الآلي من خلال كميات كبيرة من بيانات فيديو المراقبة من أجل العثور على مطابقة موضوع معين، في حين أن هذه الأساليب تقتصر حاليًّا على عوامل مثل جودة الفيديو وكثافة الحشد، مع تحسين توفير أداة أخرى مفيدة مع طرائق القياس الحيوي الأخرى والمعلومات السياقية، اطَّلع على السيناريو التالي.

وبِناء على تنبيه الإنتربول، تم احتجاز المشتبه به لاستجوابه بشكل إضافي، بَعدَ رفْضه لمناقشة هُويته أو تفسير تناقضات صورة جواز السفر، وجَّهت المديرية العامة للشرطة الوطنية التركية البيانات البيومترية الأساسية له (قزحية العين، بصمات الأصابع، ومسح الوجه) من خلال مكتب الإنتربول المحلي لتحليلها. في غضون ساعة، تم إخطار الإنتربول HQ السلطات التركية أن جواز السفر قد سُرِق منذ 6 أشهر، وذكَر الإنتربول أيضًا أن المشتبه به كان قد أعلن أنه قادم من قِبل حكومة الولايات المتحدة على أساس البيانات البيومترية لمكتب التحقيقات الفدرالي، وبناء على هذه المعلومات، طلب الملحق

القانوني الأمريكي في السفارة الأمريكية في أنقرة من السلطات التركية أن تُبقي الرجل في الحبس على ذمة التحقيق، بِناءِ على طلب من السفير الأمريكي، تم نشر قرار فريق فحص الهُوية على أساس إقليمي إلى أسطنبول لمساعدة السلطات التركية في التحقيق الجاري.



الإسناد التشغيلي

يناقِش القسم التالي التكنولوجيات الناشئة التي يمكن تطبيقُها على مهمة الإسناد العملياتي، أو ربْط الهُوية في مواقع محددة، الحوادث، والأنشطة. وتشمل هذه مجموعة متنوِّعة من المقاييس الحيوية والطب الشرعي، والأدوات التحليلية التي يمكن الاستعانة بها للمساعدة في تطوير موضوع الشخصية التفعيلي، اطَّلِع على السيناريو التالي.

في وقت لاحق بعد أربعة وعشرين ساعة، وصل فريقُ فَحْص الهوية إلى أسطنبول، وبدأ العمل بالتعاون مع السلطات المحلية، وكشفت المعلومات أن المتهم كان محتجزًا في منشأة احتجاز الولايات المتحدة في معسكر "بوكا" في العراق في عام 2008 بعد غارة العمليات الخاصة ضد منشأة لإنتاج العبوات الناسفة من المشتبه بهم، وأُطلِق سراح الرجل من قِبل السلطات العراقية بعد نحو 17 شهرًا، وحدَّدت التقرير كذلك أن الرجل هو مواطن بريطاني من أصل أردني، وأشارت المعلومات الإضافية التي قدَّمتها السلطات الهولندية من خلال الإنتربول أن الرجل كان يقيم مؤقتًا في "أمستردام" في العام السابق، ومع ذلك، غادَرَ هذا البلد، وكان يُشتَبه في مشاركته بأنه مقاتل أجنبي في سوريا، وبناء على هذه المعلومات الأولية، قدَّمت السلطات التركية إلى فريق فحص الهوية حق الحصول على الهاتف الخليوي للرجل وبنوده الشخصية.

وخلال المقابلة خضع إلى التحليل والحصول على إذن لأخذ عينات التربة وتتبُّع المواد من ملابسه، وكذلك مسحة الشدق لتحليل الحمض النووي. وقدَّمت السلطات التركية أيضًا فيديو من كاميرات المراقبة (CCTV) لوصوله وتحركاته عن طريق المطار.

على مدى العقد الماضي، كانت هناك تطورات كبيرة في استخدام تحليل الحمض النووي للوظائف العسكرية والأمنية؛ كأداة للتحقق من الهوية فإنّه يوفِّر مزايا تبدو فريدة من نوعها وغير قابلة للتغيير، مثل بصمات الأصابع، والحمض النووي الذي يُعتبر معرفة كامنة، وهذا يعني أنه يمكن الحصول عليه جنائيًّا من دون الاتصال المادي المباشر مع الشخص، كما يُقدِّم الثقة مطابقة أعلى لأي طريقة تَحقُّق من الهوية والطب الشرعي الأخرى، فعلى سبيل المثال، هناك فرصة تقرب من 86 في المئة من مطابقة البصمات الكامنة مقابل السجل في قاعدة بيانات مكتب التحقيقات الفدرالي البيومتري بشكل صحيح، على العكس من ذلك، يوفِّر الطبُّ الشرعي الحمضَ النوويَّ كضمان إحصائي مثالي للمطابقة عندما تكون العينات قد جمعت بشكل صحيح وتم معالجتها.

إن الأسلوب الأكثر شيوعا لتحليل الحمض النووي في الطب الشرعي حاليًّا، يعتبر عملية قصيرة جنبًا إلى جنب مع تكرار (STR) لتقيم مناطق STR المحددة، التي وُجِدت في الحمض النووي، يقدم STR صورة التركيب الوراثي للفرد الفريدة من نوعها، التي تقوم على مناطق الكروموسوم، وتدَّعي المكانية وجود درجة عالية من التباين بين الأفراد، ويستخدم تحليل STRعادة لسوائل الجسم، وخلايا الجلد والعظام والشعر، ويقدم وسيلة دقيقة للغاية لتحديد شخص معين كمصدر لعينة الأدلة، تحليل STR له مزاياه مقارنة مع الطرق الأخرى من حيث الحساسية، ووقت المعالجة، ومستوى أعلى من التمييز الإحصائي، بمجرد أن يتم معالجة العينة، يمكن أن تُترجم هذه البيانات إلى تنسيق رسالة CODIS المتوافقة ثم تحميلها في قاعدة بيانات الحمض النووي.

تحليل Y-STR هو طريقة مشابهة تستخدم حصرًا على كروموسوم الذكور، غالبًا ما تُطبَّق هذه التقنية للأنساب واختبار الأبوة، والاعتداءات الجنسية، المفقودين، وبعض مقاييس الذكاء، مع ذلك، يرجع ذلك إلى حقيقة أن الأقارب المتعددين يشتركون في نفس Y-DNA، ولذلك فإنّه ليس من الممكن

استخلاص التعرف الفريد من هذا التحليل، تدخل مختبرات الطب الشرعي السريع المنتشر في العراق وأفغانستان تستخدم عادة مزيجًا من هذه الطرق لتحليل الحامض النووي.

أما تقليديًّا، فكانت عملية التسلسل هي عُنق الزجاجة الرئيس للطب الشرعي الخاص بالحمض النووي، ومع ذلك، تم إدخال التحسينات، والتصغير، والتشغيل الآلي الذي قد قلَّل إلى حدٍّ كبير الكثير من هذه العقبات، التطورات الحديثة في ميكروفلويديك، والتعامل مع كميات صغيرة جدًّا من السوائل، قد أحدثت ثورة في تحليل الحمض النووي وتمكين الإنتاجية العالية للتسلسل، هذه الأساليب "الحمض النووي السريع" الجديدة تَصِف عمومًا العملية بالكامل (الأيدي الحرة) لتطوير CODIS الشخصية STR الأساسية للعينات المرجعية.

هذا وقدَّم مختلف مقدمي الخدمات التجارية أنظمةً متكاملة قادرة على أداء التحليل STR في أقل من ساعتين، ولم يتم الموافقة على تقارير الحمض النووي السريع بعد والطب الشرعي في مسرح الجريمة المحلية؛ ومع ذلك، فإنّ مختبر مكتب التحقيقات الاتحادي والوكالات الاتحادية، بما في ذلك مختبر جيش الولايات المتحدة، يقوم بإجراء الاختبار والتقييم لاعتماده في المستقبل، والاستخدام العملي.

الحدُّ الآخر للتكنولوجيات الحالية هو الحاجة إلى الفنيين المدربين الذين يعملون في بيئات المختبرات الخاضعة للرقابة؛ ومع ذلك، فالنماذج الأخيرة تتجاوز الكثير من هذه التحديات، وأحد الأمثلة الحديثة على ذلك هو نظام تسارُع معدات الحمض النووي النووية (ANDE)، وهو جهاز بحجم طابعة المكتب وقادر على معالجة ما يصل إلى خمس عينات من الحمض النووي في 90 دقيقة، والأهم من ذلك، هذا النظام يمكن تشغيله من قِبل أفراد غير تقنيين، خارج المختبر، مع إنتاج موثوق لجودة STR-التي تتوافق تمامًا مع شكل رسالة CODIS، وقد استخدمت قوات العمليات الخاصة

الأمريكية بالفعل الأجهزة المماثلة في المواقع الأمامية وفي غضون السنوات ال 5 المقبلة، نأمُل في إجراء اختبار ميداني مصغَّر، نسخة تعمل بالبطارية لقراءة الحمض النووي، والسماح للقوات بجمع الحمض النووي في بيئة تكتيكية ومقارنة النتائج على الفور مع قاعدة البيانات.

في التقدم الرئيس القادم، ستصبح أساليب جيل التسلسل القادم (الجيل القادم تسلسل الحمض النووي) تُقدِّم قُدرات جديدة وقوية باستخدام الأشكال-النوكليوتيدات الفردية (SNP) على أساس تحليل التغيرات في موقع واحد في الحمض النووي، وتنتشر هذه المواقع في أنحاء الجينوم البشري وتلعب دورًا كبيرًا في تحديد قابلية الفرد للمرض والاستجابة على اللقاحات والعوامل البيئية الآخرى، وتستخدم طرق تسلسل الجيل القادم من الحمض النووي (مجموعة فرعية من الحمض النووي في جميع الكروموسومات) لتحليل الآلاف من تعدُّد الأشكال وتحقيق مستوى أعلى من التمييز من تحليل STR الحالي، حتى للعينات المتدهورة، ويمكن لهذه التقنيات أن تساعد على التغلب على واحدة من القيود الكبيرة لتحليل STR الحالي، وتحديدًا في تحدي التعامل مع خليط من الحمض النووي، الذي يشمل المواد الوراثية للأفراد المتعددين، وهذا مصدر قلق كبير في سيناريوهات؛ مثل: مصانع (IED) العبوات الناسفة أو مسرح الجريمة؛ حيث يتعامَل أكثر من شخص مع الأدلة المادية، ويوفِّر تسلسلُ الجيل القادم من الحمض النووي قدراتٍ أكثرَ قوة لتوصيف هذه الهويات، وكذلك خفض التكلفة وسرعة التحليل.

قد أظهرت لمحات SNP المستمدة من أساليب تَسلسُل جيل الحمض النووي القادم أيضًا إمكانات كبيرة لتحليل الاختلافات بين العوامل الوراثية الفردية، وفتح الباب أمام تطبيقات جديدة وراء مُطابَقة الهُوية الأساسية، ويمكن أن تشمل اشتقاق الأصل الحيوي الجغرافي ورسم الخرائط الموسعة، والتنبؤ بالعينات الجينية، يمكن أن تكون هذه الطرق مفيدةً بشكل خاص في المناطق الجغرافية التي تُوجد فيها العلاقات العائلية والقبلية الكثيفة التي ترتبط ارتباطًا وثيقًا بالشبكات المستهدفة، وقد تم بالفعل استخدام

هذه الطرق لاستخلاص العلاقات الأسرية من عينات الحمض النووي غير المعروفة كجزء من التحقيقات الجنائية.

حتى مع زيادة القوة التحليلية للأساليب الحالية، تنميطSNP الجيني لا يزال يستخدم أقل من 0.1 في المئة من المواد الوراثية البشرية، ومع ذلك، إنَّ التقدم في التسلسل الإنتاجي العالي سوف يقدم قريبًا إمكانية تحليل الجينوم بأكمله، مما يؤدِّي إلى تحسين التنبؤ بالخصائص الفيزيائية الواضحة، المعروف أيضًا باسم الحمض النووي في الطب الشرعي، وقد أثبت تحليل الجينوم الكامل بالفعل دقة معقولة في ملامح توقع العين ولون الشعر، ويرى بعض الخبراء أنه قد يتم قريبًا توقُّع لون البَشَرة، النمش، الصلع، تجعد الشعر، وشكل الأسنان، وحتى السن.

تظاهر فريق البحث مؤخرًا بأن برنامج النمذجة ثلاثية الأبعاد قادرٌ على تصوير "الوجه وراثيًّا" على أساس مزيج الجنس ونسب تحديد الحمض النووي، ويمكن بعد ذلك أن يتم تكرير الصورة على أساس 20 من 24 من المتغيرات الجينية المعروفة بالمشاركة في الاختلاف في الوجه، في حين أن مثل هذه الطلبات لا تزال جديدة، مثيرة للجدل، ولا تجوز في معظم الإجراءات القانونية.

وقد انخفض تعقيد حساب تسلسل الجينوم الكامل بشكل كبير في السنوات الأخيرة من ملايين الدولارات قبل عقدٍ من الزمن إلى بضعة آلاف في الوقت الحاضر، بالإضافة إلى مجموعة واسعة من التطبيقات الطبية، أن هذه القدرة تُقدِّم تقنيات محسَّنة للتحليل الجيني، أو تفسير تعبيرات الجينات التي يسببها التعرض البيئي المحدد للمواد الكيميائية، والإشعاع، أو غيرها من العوامل، وهذا يمكِن أن يؤدِّي إلى ملامح سِمة الشخص الأكثر تفصيلًا التي تَستنِد إلى شيء أكثر من الحمض النووي المتبقي، التطبيق الآخر يمكن أن يكون ناشئًا من تسلسل الجينوم الكامل، الذي يكون له قدرات قوية لتحليل ما وراء

الجيني من المواد التي تم الحصول عليها من العينات البيئية، هذا يمكن أن يوفِّر خصائص فريدة من البيئات الميكروبية، على سبيل المثال، تحليل التحركات الأخيرة للشخص بناء على أدلَّة من التُّربة النادرة، الكائنات الميكروبية، أو عينات حبوب اللقاح، هذا ويمكن أيضًا أن يُستخدَم لكشف التعرض الأخير للمواد الكيميائية، اطلع على السيناريو التالي.

مع استمرار التحقيق، حصل فريقُ فَحصِ الهُوية على النتائج الأولية من تحليل الحمض النووي، وتَطابَق ملفُّ المشتبه فيه مع العيِّنة مجهولة الهوية المفهرسة في أواخر عام 2009 من الأدلة الجنائية التي عُثِر عليها في مصنع العبوات الناسفة في العراق، بعد عدة أيام، تلقى الفريق نتائج تحليل العينات من الطب الشرعي التي تم الحصول عليها من أثر ملابس المشتبه به، تم تحديد أن التربة المجففة على حذاء الرجل واللقاح في ملابسه يتَّسق مع قوام التربة وأنواع النباتات الشائعة في شمال سوريا، مما يشير إلى السفر الأخير إلى تلك المنطقة، وقد تم تأييد هذه الشبهة من استغلال الهاتف الخليوي الذي وفَّر الوقت ومواقع سفر المشتبه به الأخيرة، ويتضمَّن الهاتف الخليوي أيضًا معلومات تعريف الشخصية لعدد من المقربين، بما في ذلك الأسماء والعناوين وأرقام الهاتف وعناوين البريد الإلكتروني وأسماء الدردشة المستخدمة، وتبادُل الرسائل النصية الأخيرة مع أشخاص يُشتَبه في أن لهم صلات بشبكة التسهيلات للمقاتلين الأجانب المعروفين، احتوى المتصفح أيضًا على رقمٍ قياسيٍّ من عدة مواقع من وسائل الإعلام الاجتماعية التي تم الوصول إليها مؤخَّرًا، وتم استخراج عدد من أشرطة الفيديو القصيرة من ذاكرة الهاتف؛ ليتمَّ تحليلها ومقارنتها مع عيِّنات وسائل الإعلام الأخرى التي نشرت على منتديات شبكة الإنترنت التي يرتادها مجتمع المقاتل الأجنبي، بالإضافة إلى ذلك، تم استخدام بيانات الاستشعار الداخلية للهاتف لإنشاء ملف تعريف بيومتري من الأنماط المخزنة والتاريخ، واستنادًا إلى هيئة تطوير الأدلة، طَلَب الملحق القانوني بالولايات المتحدة من السلطات التركية أن تواصِل حبس المتهم مع استمرار التحقيق.

رسم خرائط الشبكة

بمجرد إنشاء التاريخ التشغيلي، تتضمَّن الخطوة التالية الربط بين الهوية والأنشطة الأخرى، والمواقع، وشبكة واسعة من الجهات الفاعلة ذات الصلة. واحدة من التحديات التحليلية الرئيسة في هذه المهمة هي كشف شبكة الاتصالات الضمنية الواردة في كميات هائلة من البيانات غير مهيكلة، كما أوضح مديرُ الاستخبارات الوطنية "جيمس كلابر" في الآونة الأخيرة، في عصر البيانات الكبيرة، إن التحدي هو العثور على الإبر دون الاضطرار إلى التعامل مع أكوام التبن، ويكشف القسم التالي بعضَ التطورات الحديثة في مجالات مثل: تحليلات الفيديو، ومعالجة اللغة الطبيعية، وإدارة البيانات، واستكشاف على وجه التحديد كيف يمكن لهذه التقنيات أن تحسِّن طرقَ الفرز وربط وتحليل المعلومات من مصادر متنوِّعة، اطلع على السيناريو التالي:

مع استمرار التحقيق، اقترح تحليل الحمض النووي للقرابة مقارنة مع قاعدة بيانات CODIS للارتباط العائلي المحتمل بين المشتبه به الذي اعتقل في تركيا، والرجل الآخر الذي اعتقل مؤخرًا خلال غارة مكتب التحقيقات الفدرالي ضد الخلية الإرهابية في أتلانتا، جورجيا، واتهمت الخلية بإدارة التخطيط السابق لتفعيل الهجوم المحتمل ضدَّ مبنى الاتحادية الأمريكية.

وتضمَّنت موادَّ جهاز الكمبيوتر المحمول من خلال قوات الدفاع الشعبي، وملفاتٍ تحتوي على الملاحظات المكتوبة بخط اليد وتعليمات صنع القنابل. وتشير الكتابة وتحليل المحتوى من ملفات المستندات إلى وجود عدة وثائق في ملفات المشتبه به في تركيا، وقد ضبط الكمبيوتر المحمول خلال غارة

أتلانتا التي تتضمَّن أيضًا العديدَ من مقاطع الفيديو، التي اتُّخذت في معسكر تدريب إرهابي مجهول الهوية، تحليل التحكم في لقطات مطابقة شرائح الفيديو التي تم الحصول عليها من الهاتف الخليوي الخاص بالمشتبه به، مما يدل على أن شخصًا قد قام باستخدام كاميرا الهاتف التي قد سُجِّلت كلٌّ من أشرطة الفيديو في معسكر التدريب، تحليل محتوى الفيديو، بما في ذلك الأنشطة والمناظر الطبيعية، والأفراد، وأيضًا مُطابَقة الفيديو المماثِل الذي نُشِر على عدة مواقع بوسائل الإعلام الاجتماعية التي يرتادها الجماعات المتطرفة، من هذه البيانات والمعلومات الداعمة الأخرى، وقد ضاق موقع المخيم لعدد قليل من المواقع المحتملة، وتقدِّم هذه المواد أيضًا أدلَّة على الصلة التشغيلية المباشرة بين المشتبه به في السجن التركي وخلية التخطيط في أتلانتا.

شهدت السنوات القليلة الماضية تقدمًا كبيرًا في تحليلات الفيديو، وخاصة استخدام الذكاء الاصطناعي لتحسين تحليل المحتوى، يركِّز مجال "رؤية الكمبيوتر" على هذه الطرق الآلية للتجهيز، والتفسير، وتحليل محتوى الصورة. ومعظم الطرق التقليدية لفرز وربط بيانات الفيديو كبيرة الحجم لا تزال تعتمد على المعلومات الوصفية مِثل: عناوين وتعليقات النص المرتبطة مع وسائل الإعلام بدلًا مِن المحتوى الفعلي، وهذا يمثل تحديًا كبيرًا لإجراء استرجاع البيانات والوسائط المتعددة على نطاق واسع، الاستفسارات، والتحليل القائم فقط على الكلمات الرئيسة الوصفية، إن المقاربة الأخرى لاستخدام التحليل الدلالي القائم على نموذج تحديد المحتوى تتَّصِل بمجموعة محددة سلفًا من الأنشطة، كما هو الحال مع غيرها من المهام التي تنطوي على النمذجة الاحتمالية المعقدة، كانت HMM والأساليب المتعلقة هي نهج واحد لإدراك نمط محتوى الفيديو.

يهدف الذكاء الاصطناعي وأساليب التعلم العميق لتحسين التحليل القائم على المحتوى، ومساعدة اكتشاف العلاقات السياقية بين البيانات والفيديو ووسائل الإعلام الأخرى، والمعلومات، وتتعلَّق إحدى

المظاهرات الأخيرة بتدريب الكمبيوتر للتمييز بين مجموعة من رجال لعب الفريسبي وقطيع من الفيلة التي تمشي على العشب، في حين تبدو مهمة أساسية للإنسان، وهذا يمثِّل إنجازًا تقنيًّا رئيسًا لأجهزة الكمبيوتر، وتطوُّر هذه الأدوات سيكون حاسمًا للفهرسة، وتحليل الملايين من الصور الرقمية وملفات الفيديو التي تم إنشاؤها وتحميلها على شبكة الإنترنت كل يوم، وهو المبلغ الذي يتجاوز بالفعل إلى حدٍّ كبير ما يمكن القيام به من خلال التحليل البشري بسرعة، وقد يظهر أحد الأمثلة من أجل تسليط الضوء على الإمكانات الكبيرة في هذا المجال مؤخرًا في التطبيق التجاري، باستخدام برنامج التعلم العميق لتحليل أشرطة الفيديو بسرعة والتعرف على حوالي 10،000 من الأشياء والأنواع المختلفة للمشاهد ضمن مجموعة من المقاطع، ويتمكَّن البرنامج من استخلاص وتحديد المفاهيم الوصفية المجردة مثل "المتعة".

وتتمثَّل أحدُ التحديات التحليلية ذات الصلة، التي تتعلق بأجهزة الكمبيوتر مع التدريب على تفسير واستخراج مَيْزات المحتوى المختلفة بعض الشيء مثل: الأدوار الاجتماعية المحددة، على سبيل المثال، أظهر النموذجُ الأخيرُ القدرةَ على التعرف على الشخص الأكثر أهمية من بين مجموعة من الناس الذي تم ظهورهما معًا في صورة، هذا النوع من المهمة يعتمد على استنباط المعنى الدلالي المعقد من الإشارات البصرية الخفية، ثم ترجمة هذه المؤشرات البصرية في وصف النص المفيد الذي يمكن فَهْمه من قِبل البشر أو المستخدم في التحليل الحسابي، وقد وجد الباحثون في جوجل مؤخرًا أن مِثل هذا الأسلوب يقوم بترجمة الصور المعقَّدة إلى جملٍ وصفية قصيرة، ويُشارك النهج في شبكات التدريب العصبية على مهمتين مُنفصلتين، ولكن ذات الصلة: أولًا، معالجة الصور في التمثيل الرياضي على أساس المحتوى، ثم، ثانيًا، ترجمة هذه المعلومات إلى نصٍّ قابل للقراءة، في هذه الحالة، تُطابِق الشبكة العصبية عشرات الآلاف من الصور التي تم تحديدها بالفعل مع الأوصاف المكتوبة من قِبَل البشر.

هناك الأعمال ذات الصِّلة في هذا المجال على الأساليب المحسِّنة لمصادقة الوثائق وتحديد مصدر الصورة، وهي أداةٌ مفيدة بشكل خاص؛ نظرًا للأمثلة الأخيرة من التلاعب بالصورة التي يتم استخدامها كجزء من الحملات الإعلامية، على سبيل المثال، خلال الهجوم عام 2014 من قبل الدولة الإسلامية في العراق، بثَّ النشطاء صورًا لطائرات الهليكوبتر والدبابات التي يفترض أنها قد التُقِطت من قِبل قوات الأمن العراقية، ومع ذلك، كشف التحليل في وقت لاحق أن العديد من الصور المنشورة على مواقع وسائل الإعلام الاجتماعية تبيِّن أن الصور لكبار السن، وقد استخدمت إيران وروسيا، وغيرها أيضًا صور التلاعب بغرض التضليل والخداع.

ومن بين الجهود المبذولة التي تركِّز على التغلب على هذه التحديات هي المشاريع البحثية الأخرى لبرنامج الاستخبارات المتقدم "الكشاف" المصمم لمساعدة المحللين لتحديد موقع الصور، غير مضاف إليها العلامات الجغرافية من مجموعات الصور أو مقاطع الفيديو، هذا ويمكن الاستفادة من أدوات جمع المصادر على شبكة الإنترنت أو استخدام تقنيات الصورة المطابقة على أساس قواعد البيانات المرجعية الكبيرة من الصور العامة والأرضية، بما في ذلك ميزات مِثل ارتفاع البيانات والجيولوجيا السطحية، والغطاء النباتي الأرضي، الجغرافيا المحلية، والمعلومات الثقافية التي تعتبر جزءًا لا يتجزَّأ، وقد أثبتت تجارب النموذج بعض النجاح الأولي باستخدام الفيديو وصور ملفات البيانات الغنية التي تحتوي على ميزات التعرف نسبيًّا، ومع ذلك، في حالة المناطق النائية مع البيانات الأقل جزء لا يتجزَّأ، ولا تزال الأدوات قادرة على تضييق منطقة البحث في بعض الحالات.

كما هو الحال مع بيانات الصور والفيديو، والنمو المتسارع لملفات التوثيق والإعلام الذي يستند إلى نص تحديات التقنية المماثلة للمحللين. هذا هو المحور العام وتكنولوجيات معالجة اللغة الطبيعية (NLP) ، يتعامل مجال علم الحاسوب مع مهمة تمكين أجهزة الكمبيوتر لاستخلاص المعنى من مدخلات اللغة

البشرية، وتَمَسُّ البرمجةُ اللغوية العصبية العديدَ من المجالات الوظيفية التي نُوقِشتْ بالفعل، بما في ذلك المهامُّ مِثل التعرف على الكلام، الترجمة الآلية، وتصنيف الوثيقة الآلية. كما هو الحال مع تحليل الصور، والقدرة على استنباط المعنى السياقي من كميات كبيرة من البيانات غير مُنسَّقة وملفات الوسائط، وهو أمر حاسم لاكتشاف كِيان وشبكة رسْم خرائط العلاقات.

قد تمَّ تطبيقُ نهج البرمجة اللغوية العصبية التقليدية على نهج التعلم الآلي والنماذج الإحصائية، لاتخاذ القرارات الاحتمالية على أساس المقارنات إلى الإحضار من النصوص العيِّنة المتاحة في قواعد البيانات الرقمية ومجموعات الإنترنت، هذا هو في الأساس كيفية عمل الصوت وتطبيقات ترجمة جوجل، من خلال إجراء المقارنات إلى الوثائق المترجمة سابقًا التي وجِدت في جميع أنحاء الشبكة، يتم تحويل مدخلات اللغة الطبيعية إلى مجموعات البيانات المتجانسة، وهذا يتيح سهولة اكتشاف سِمات الهوية واستخراج العلاقة.

كما هو الحال في المناطق الأخرى، التقدم في الاصطناعية يُظهِر وعود المخابرات الكبيرة لتحسين دقة أساليب البرمجة اللغوية العصبية، وخاصة في مجالات استرجاع المعلومات وارتباط البيانات، والأهم من ذلك، تذهب العديد من هذه التقنيات إلى ما هو أبعد من الترجمة الآلية الأساسية والتعرف الضوئي على الحروف، وهذه الأساليب قد تمكِّن قريبًا أجهزة الكمبيوتر من استخلاص المعنى الدلالي ومستوى الوظائف العالي الأكثر عمقًا؛ مثل: تحليل المشاعر وتصور البيانات المتقدمة على أساس الروابط التي تُعتَبر جزءًا لا يتجزَّأ من بين الناس والأماكن والأنشطة الواردة في كميات كبيرة من البيانات غير المهيكلة.

بعض التطبيقات الحالية ظهرت بالفعل في القطاع التجاري، على سبيل المثال، استخدام أساليب البرمجة اللغوية العصبية لتفسير مدخلات وسائل الإعلام الاجتماعية والتوصية المنطقية المناسبة والأساليب المحسِّنة لفَهْم نيّات المستخدم الضمنية وراء سلسلة من الكلمات، التي دخلت في محرك البحث، وقد

طبقت شركة الذكاء الاصطناعي تقنيات البرمجة اللغوية العصبية لتمكين التحليل في الوقت الحقيقي لقنوات الاتصال المتعددة، بما في ذلك مواقع الأخبار، ومنتديات الإنترنت، وسائل الإعلام الاجتماعية للمساعدة في تحديد الإتجاهات الناشئة والأنماط السلوكية الفريدة من نوعها، والأهم من ذلك، أن هذه النُّظم تتَّجِه نحو القدرة على استخلاص المعنى السياقي دون الحاجة إلى المحلل البشري، فكلٌّ من المخابرات ومشاريع البحوث المتقدمة لوكالات الدفاع لديها برامج متعددة في هذا المجال، وتُحاوِل تطبيق هذه التقنيات لاستخدامها. اطلع على السيناريو التالي:

خلال الأسابيع القليلة المقبِلة، تمَّ مواصلة التحقيق مع التحليل الرقمي للمشتبه به من خلال نشاط وسائل الإعلام الاجتماعية، وتصفُّح التاريخ، والاتصالات التي تم الحصول عليها من بيانات الهاتف، وكشف هذا التحليل عدة روابط مفيدة بين مختلف التشكيلات على الخط، الوظائف المضاف إليها العلامات الجغرافية والصور ومحتوى الفيديو، قدَّم ارتباطًا هذه التوقيعات الرقمية النمط الأساسي للحياة على أساس الأنشطة الأخيرة، والمواقع، والتفاعلات، والاتصالات من خلال مختلف القنوات الإعلامية والاجتماعية، كما أُعيد بناؤها فريق خريطة الهُوية الرقمية للمشتبه فيه، كانوا قادرين على استنتاج الشبكات الاجتماعية الكامنة على أساس العلاقة مع المستخدمين الآخرين الذين يشاركون الأنماط المماثلة، والعادات، والمواقع، والمحتوى الدلالي للمحققين.

واقتُرِح هذا الدليل وصلات إلى عدة نقاط رئيسة للشبكة لتقديم التسهيلات للمقاتلين الأجانب وموقع منشأة المعالجة، التي لم تكن معروفة سابقًا للمجنَّدين الذين يصلون حديثًا، فمزيد من التحليل من أشرطة الفيديو الدعائية التي تم نَشْرها في عدة مواقع لوسائل الإعلام الاجتماعية قامت بإنتاج احتمال إضافي عالٍ من المطابقة مع صورة الوجه، المشية، ونبرة صوت المشتبه به، وبشكل منفصِل أشارت نتائج تحليل

جينوم الحمض النووي الكامل إلى احتمال تعرُّض المشتبه به في الآونة الأخيرة إلى السلائف الكيميائية المستخدمة عادة باسم المسرعات لصنع القنبلة.

يتناول القسم الأخير كيف تُقدِّم الأدوات التحليلية لوسائل الإعلام الاجتماعية وغيرها من "البيانات الكبيرة" قدراتٍ جديدة لربْط توقيعات الهوية لهياكل شبكة أكبر، وربما تمكّن الأساليب المحسنة للتحليل التنبؤي، ويُقدِّم تحليل وسائل الإعلام الاجتماعية وسيلةً أخرى لاكتشاف الهوية ويَعزو عددًا من الأسطر عبر الشبكات على نطاق أوسع، إن النهج في هذا المجال يقوم على دراسة تحليل الرسم البياني، مجال متعدِّد التخصصات المعنيَّة مع استخراج المعلومات، وإدارة البيانات، والتصور، وتشمل هذه المهام استخدام الأساليب الإحصائية للكشف عن الهياكل الضمنية للشبكة، سمات الفاعل، والعلاقات المضمنة.

بعض العوامل المعقدة في هذا التحليل تشمل التعامل مع الذاتية الكامنة في البيانات النصية والهويات الغامضة، وعدم اليقين في تصنيف العلاقات بين هذه الكيانات، وقد تمَّ العثور على العديد من هذه الأدوات المتطورة لتحليل وسائل الإعلام الاجتماعية في القطاع التجاري، ويتم استخدامها حاليًّا لأغراض مِثل: التسويق والتنبؤ السياسي، ومع ذلك، فإنّ العديد من هذه الأدوات كانت تطبيقات ذات استخدام مزدوج للأمن القومي والإغاثة من الكوارث، ومهام إنفاذ القانون، على سبيل المثال، تم استخدام التطبيقات القادرة على تحديد مواقع تُغذِّي الصوت ووظائف الفيسبوك لتحليل الأنماط السلوكية وسمات الهوية من الجهات الفاعلة لوسائل الإعلام الاجتماعية المجهولة.

إن البعض الآخر من الباحثين في مجال تحليل وسائل الإعلام الاجتماعية قادرون على بناء الهُوية الشخصية العامة على أساس معلومات السمة الضمنية التي تُعتبر جزءًا لا يتجزَّأ داخل محتوى وهيكل

شبكة الاتصالات؛ مثل: الأنماط اللغوية، العلاقات الاجتماعية، والأفضليات المعبَّر عنها، على سبيل المثال، أظهر الباحثون أن سِمات الهوية؛ مثل: العمر والجنس والمهنة والتعليم، وحتى السمات الشخصية، يمكن التنبؤ بها بدقة من خلال تحليل نشاط تصفُّح الإنترنت، وقد أظهرت دراسات أخرى كيف يمكن لأنماط وسائل الإعلام الاجتماعية أن تكشِف بدقة خصائص مثل الميول الجنسية أو العرق، والآراء الدينية والسياسية، في حين لم تحدِّد بشكل واضح أن نقاط هذه البيانات توفِّر أساسًا قويًّا لتحديد ملامح وفَرْز الهُوية الأساسية، لقد استغلّ العملُ المتعلق بمحتوى الوسائط الاجتماعية لتوليد تنبؤات موثوقة نسبيًّا للتعرف على صفات الشخصية؛ مثل:

الانبساط، العصابية، القابلية، الضمير، والانفتاح.

ويستند جزء كبير من هذا العمل على رؤى جديدة حول كيف تخلُق بنية الشبكة الاجتماعية للفرد "البصمة الرقمية" التي في بعض الحالات، يمكن أن تتنبَّأ بسمات الشخصية الكامنة والنزعات السلوكية؛ مثل: نجاح العمل، وتعاطي المخدرات، والخيانة، والمستوى العام للسعادة العاطفية، وقد طبَّق الباحثون أيضًا التحليل الإحصائي العلائقي لتحسين التنبؤ بالسمة والتصنيف على أساس مدى المتغيرات المحددة، التي تنتقل بين الأفراد على أساس العلاقات الاجتماعية والتنظيمية، على سبيل المثال، تم استخدام هذا النوع من التحليل لتحديد النزعات السلوكية من الجهات الفاعلة الفردية داخل المجتمعات الاجتماعية الأكبر، وتستخدم لمهام مثل الفحص التنبؤي على أساس المخاطر، وعلى سبيل المثال، وُضِع برنامج الفحص الحكومى البريطاني لمنع نموذج المؤشرات السلوكية كجزء من إطار تقييم ضَعْفها، تطبيق 22 من المتغيرات المرتبطة بعوامل مثل المشاركة، والقصد، والقدرة، هذه المؤشرات معًا يمكن أن تُوحي بضعف الفرد تُجاه الانجراف نحو التطرف العنيف.

قد تم إيضاح الكثير من المعلومات اللازمة لهذا التحليل من بيانات وسائل الإعلام الاجتماعية المتاحة علنًا والمصادر المفتوحة الأخرى، مؤخرًا، قام فريق من مركز الكلية الدولية لدراسة التطرف والعنف السياسي (ICSR) باستخدام معلومات وسائل الإعلام الاجتماعية والبيانات الأخرى المفتوحة لبناء لمحات من نحو 700 مقاتل أجنبي غربي من الذين سافروا إلى سوريا كمقاتلين، وتجميع أكبر عدد ممكن نحو 72 من نقاط البيانات لكل فرد. هذه البينات تقدِّم أفكارًا مفيدة في الهويات الشخصية والعملية للأفراد للانضمام إلى الحركة، فضلًا عن التفاصيل الهامة حول طرق ومسارات تجنيدهم، مِن الجديرِ بالذِّكر، أن هذا الدليل قد أنشأ أفواجَ المقاتلين الأجانب التي تتطوَّر من مجموعات من الأصدقاء الاجتماعية، التي تحديدها بوضوح عادة واستخلاصها من مناطق جغرافية واحدة.

هذا المثال يُبرز أحدَ التطبيقات الكلاسيكية لنظرية الشبكة الاجتماعية، وتحديدًا في ديناميات التأثير الاجتماعي، وقد أظهرت الأعمال الأخيرة في هذا المجال كيف يمكن لهذه التقنيات تحديدَ قيادة الجهات الفاعلة والأدوار الوظيفية بين أعضاء الشبكة، التي تستنِد فقط على الأنماط العامة للنشاط، والاتصالات، والصفات الفردية، وقد أثبتت المجالات ذات الصِّلة من البحث أيضًا كيفية تحليل الشبكات الاجتماعية، التي يمكن استخدامها للكشف عن الخداع، إسناد التأليف، تحليل المشاعر، وتعديل الرأي، وهذا مماثل لفكرة "حشد الاستشعار" أو باستخدام البيانات المجمعة المستمدَّة من الأجهزة المحمولة لنموذج الأنماط السلوكية العامة، وكذلك توقُّع متغيِّرات أكثر تحديدًا من الفائدة، ويمكن أيضًا لهذه الأساليب تقديمَ مناهج جديدة لتحليل الشبكة الاجتماعية الحيوية، وتُعتبر أحد الفروع التي تدرس التغيرات في السلوك من الشبكات الاجتماعية على مر الزمن، أداة هامة للكشف عن السلوك الشاذ داخل الشبكات وبين الجهات الفردية التي تعمل داخلها.

قد وفَّر الصِّراع الدائر في سوريا مجموعةَ بيانات غنية للتَّجريب، منذ بداية الأعمال العدائية خَلَق المقاتلون الأجانب ملايين من مشاركات وسائل الإعلام الاجتماعية وكميات هائلة من المحتوى الرقمي، حسب بعض التقارير، فإنَّ الدَّولة الإسلامية التي ترتبط ببعض الوظائف تُرسل حوالي 90000 رسالة كل يوم، تنطوي على ما يصل إلى 30،000 أتباع نشطاء في جميع أنحاء العالم. فريق واحد من الباحثين استخدم مؤخرًا هذه البيانات لتطوير تمثيل الشبكة المفصلة للديناميكيات الطائفية المتورِّطة في الصراع، وكشف هذا التحليل على مستوى مذهل من التعقيد الداخلي بين الفصائل، بما في ذلك الانقسامات الضمنية بين أطراف النزاع التي لم تكن واضحة من التقارير القصصية، والأهم من ذلك، حدَّد هذا التحليلُ أفواجًا متميزة من أتباع وسائل الإعلام الاجتماعية لمراقبة الصراع من خارج سوريا وتوفير نظرة ثاقبة لديناميات الحملة الإعلامية الخارجية.

تقريبا كل هذه التقنيات التحليلية قائمة على استخدام "البيانات الكبيرة" لاكتشاف الهوية وعلاقة السمة، يشير هذا العام، وغالبًا ما يساء استخدامها، وعلى المدى ليس فقط لحجم مجموعات البيانات، ولكن أيضًا إلى الأدوات الحاسوبية والأساليب الإحصائية المستخدمة لاستخلاص المعنى من البيانات. التعامل مع تنوُّع وحجم المعلومات الواردة في هذه المجموعات الضخمة قد خَلَق وضعًا غير "ساحق وغير مفهوم للإنسان"، ويتطلب تحسين المنهجيات لتحويل هذه البيانات إلى معلومات متماسكة، البعض قد تم وصفها بالفعل في طول هذه التقنيات، ومع ذلك، بعض الأمثلة توضِّح كيف يمكن لهذه المجموعات الكبيرة من البيانات التي يمكن استخدامها في المستقبل تحسين اكتشاف الهوية والإسناد العملياتي، ورسم خرائط الشبكة.

أحد الأمثلة الأخيرة على أداة "البيانات الكبيرة" هو محرِّك البحث ميمكس برعاية DARPA. ويَستنِد هذا التطبيق إلى الرسوم البيانية التي تعتمد على العلاقات بين صفحات الويب، وتحديدًا أولئك

الذين يقيمون في ما يسمَّى شبكات "ظلام الويب" حيث يتم حَجْب عناوين IP، على عكس محركات البحث القياسية المصممة للتدقيق من خلال النصوص والصور، يستخدم ميمكس جزءًا لا يتجزَّأ من المعلوماتِ؛ مثل: الإحداثيات الجغرافية التي يُرمَز إليها في الصور والأرقام المكتوبة بخط اليد داخل الصور، وحتى المشاهد الخلفية من الصور التي يمكن مقارنتُها بشكل مستقلٍّ عن غيرها من الأشياء في الصورة، من هذه المعلومات ميمكس تَنتج تخطيط الشبكات على أساس العلاقات الضمنية التي تعتبر جزءًا لا يتجزَّأ من ضمن البيانات غير المفهرسة، بما في ذلك أشياء؛ مثل: أرقام الهواتف وعناوين الشوارع، والأسماء الفردية.

مثال آخر على مشروع البيانات الكبيرة؛ وهو قاعدة البيانات العالمية للأحداث، لغة ولهجة (GDELT)، في جميع أنحاء العالم، منذ عشرات السنين، المرجعية الجغرافية، بيانات الحدث اليومي GDELT، يتم مراقبة المطبوعات والإذاعة، ومصادر وسائل الإعلام في أكثر من 100 لغة، عبر كل بلد في العالم، وذلك باستخدام تكنولوجيا الترجمة الآلية للوصول إلى مصادر غير الإنجليزية، الهدف من المشروع هو الكتالوج الإنساني، والسلوكيات المجتمعية على نِطاق واسع وصولًا إلى المستوى الجزئي، على سبيل المثال، إنه يمكن استخدام الدرجات من مجال البيانات للحصول على كل التفاصيل المتاحة حول حدث معين مثل هجوم إرهابي صغير، والجهات الفاعلة الفردية المعنية، وأدوارهم.

قد تم وضْع مثال آخَر لدراسة المجموعات العنيفة مع قاعدة بيانات تحتوي على معلومات مُفصَّلة عن حوالي 223،000 من حوادث التطرف العنيف والجريمة، التي تَضُمُّ أكثر من 43،000 من الأفراد مع اتصالات إلى أكثر من 3000 من جماعات العنف، وتستند هذه البينات على وسائل الإعلام التقليدية ووسائل الإعلام الاجتماعية، ومحتوى الفيديو، تقارير الشرطة، وثائق المحكمة، من بين مصادرَ أخرى،

وبنية قاعدة البيانات تحتوي على ما لا يقل عن 1500 من المتغيرات للمساعدة في تصنيف الأحداث الفردية ثم تصور الروابط داخل البيانات.

بعض تطبيقات "البيانات الكبيرة" قد تُقدِّم في نهاية المطاف أساليب محسنة للتحليل التنبؤي، تتجاوَز استهداف الأفراد التي تم تحديدها بالفعل كمصدر للتهديد، على سبيل المثال، إنها قد تكون قادرةً على توفير وسيلة لكشف جهات محدَّدة استباقية أو تسليط الضوء على الظروف البيئية التي هي أكثر عُرضة لإنتاج التطرف لدى بعض الأفراد، على سبيل المثال، مشروع قاعدة بيانات الإرهاب العالمي في جامعة "ميريلاند" يحتوي على سجلات مفصَّلة لحوالي 125،000 من الحوادث الإرهابية، التي يعود تاريخها إلى عام 1970، وذلك باستخدام 40-120 من المتغيرات لكل سجل حادث، من داخل هذا الملف، قد طوَّر الباحثون مجموعةَ بيانات أكثر تفصيلًا حول 1500 من الأشخاص الذين اتَّجهوا نحو التطرف العنيف وغير العنيف في الولايات المتحدة منذ الحرب العالمية الثانية، بما في ذلك معلومات حول السيرة الشخصية، والسجلات الجنائية، والشبكات الاجتماعية، والتواريخ الشخصية، وقد مكَّنت هذه البيانات الباحثين من تحديد بعض الخصائص المشتركة المهمة بين المجموعة بما في ذلك أهمية الشبكات الاجتماعية في وجود الوسطاء الرئيسين، ولكن أيضًا المتغيرات مِثل العمر والحالة الاجتماعية، والمقاييس تُعتبر عاملًا للاستيعاب الاجتماعي.

بينما وعْد النقاد بالبيانات الهائلة كان في ذُروته على الدوام، ومن المرجح أن يقدم واحدة من عدد قليل من البدائل القابلة لتطبيق نماذج التنميط والمؤشرات السلوكية المرتبطة بالفرز على أساس الهوية، وكذلك يحتمل أن تكون دعمَ استراتيجيات التدخلات الوقائية قبل الاغتراب الاجتماعي، الذي يحرك الجهات الفاعلة الفردية نحو التطرف والعنف؛ اطلع على السيناريو التالي:

مع استمرار التحقيق، مع تحليل شبكة التواصل الاجتماعي للمشتبه به تم ايجاد العشرات من خيوط التحقيق في الولايات المتحدة والعديد من الدول الأوروبية. وأكَّدت الروابطُ تورطَ المشتبه به مع الجهات

الفاعلة الأخرى المعروفة؛ لتكون جزءًا من شبكة التسهيلات للمقاتلين الأجانب المسؤولة عن تجنيد ونقل مقاتلين جدد إلى نقطة الدخول الأولى في سوريا من أجل التلقين والتدريب، دَفعت هذه الخيوط عدَّة تدخلات وقائية تركِّز على الأفراد بالفعل في خط التوظيف، استغلال الصور والمحتويات الإضافية الناتجة عن مشاركات وسائل الإعلام الاجتماعية تُقدِّم دليلًا على أن تضيق الخناق على أي موقع ممكن من مواقع التدريب السوري، وحددت العديد من الأفراد الآخرين العاملين في الموقع، واستنادًا إلى البيانات الشخصية التفعيلية للشخص والدليل الهام للعلاقات الشخصية إلى شبكة المقاتلين الأجانب، تقدَّمت الحكومة البريطانية باتهامات جنائية ضد الفرد، وبدأت في طلب رسمي مع السلطات التركية.



رسم تقييم الحرب الإلكترونية 1.0

السيناريو السابق ومناقشة مَسْح جزء صغير من مشهد التكنولوجيا الناشئة، يعتبر الطريقة التي يمكن أن تستخدم بها هذه الأدوات لشن الحرب الإلكترونية في المستقبل، كان هذا الاستكشاف متضاربًا بدلًا من كونه تنبؤي، وأقرَّ بالطبع تأكيدَ الابتكار التكنولوجي وطبيعة الديناميكية العالية في بيئة التهديد، هذه العوامل تُبرز التحديات الهائلة التي تواجِه المخططين العسكريين وصنَّاع القرار؛ لأنها محاولة لمواءمة الاستراتيجية الدفاعية مع أهداف البحث والتطوير، التي تُركِّز على المخاطر على الأرجح، واللمحة المستقبلية للأمن القومي الأمريكي.

وفي هذا المعنى، فإنَّ قصة الحرب الإلكترونية قد تكون حكاية تحذيرية حول أخطار التنبؤ في غير مَحلِّه من التهديدات المستقبلية والتقنيات اللازمة لإلحاق الهزيمة بهم، فكثيرا ما وصفت هذه الدراسة تطور التصميم، ولكن بدلًا من عقد إعلان التعديلات المخصصة للاستجابة للمقتضيات التي تم إنشاؤها من قِبل عدو غير متوقَّع، فإن هذا الوضع يتطلَّب من جهاز الأمن القومي الأمريكي إعادة التوجيه بسرعة على نوع جديد من التهديد، ثم تطوير مذاهب الدعم والتقنيات والأساليب اللازمة لمواجهة هذه التحديات.

أن كلًّا من الجيش وأجهزة الاستخبارات، والكيانات الأمنية المحلية قادرة على التعرف على ما إذا كان هناك حاجة في نهاية المطاف إلى وضع هذه الخطط موضع التنفيذ كشهادة على الإبداع وتفاني هذه المنظمات والأفراد، ومع ذلك، فإنّه يسلط الضوء أيضًا على التكلفة الباهظة وخطر اتِّخاذ قرار خاطئ؛ كما يشير مفهوم تفعيل الجيش الأمريكي إلى:

التفكير بوضوح حول النزاع المسلح في المستقبل يتطلَّب النظر في التهديدات، والأعداء والخصوم، والبعثات المتوقعة والتكنولوجيات الناشئة، وفرص استخدام القدرات الموجودة بطرق جديدة، والملاحظات التاريخية والدروس المستفادة. حتى في ظلِّ أفضل الظروف، وهذا يمثِّل مهمة صعبة.

في تقييم الأهمية الكبرى للحرب الإلكترونية، ينبغي توضيح عدد قليل من التعاريف. مصطلح "الحرب" يصف الطريقة التي تتبعُها دول الحرب، وتحديدًا في الأدوات والتقنيات وأساليب تطبيق القوة القسرية ضد العدو في ميدان المعركة، تمتد من هذا، فإنَّ "طبيعة الحرب" تَصِف هذه الظاهرة سياق الحرب داخل محيط أكبر من التأثيرات الثقافية والتكنولوجية والاجتماعية والسياسية والبيروقراطية، صعود الحرب الإلكترونية يعكس تغييرًا كبيرًا على المستويين من التحليل؛ كنموذج جديد من الحرب، شكَّلت الحرب الإلكترونية مجموعة متميزة من الأدوات والتقنيات والأساليب التي تطوَّرت على مدى فترة قصيرة نسبيًّا من الزمن من النظرية إلى التطبيق في استجابة مباشر على التحديات التشغيلية المحددة على أرض المعركة، هذه التحديات التي تركِّز في المقام الأول على مهمة محاربة العدو كما نَظَّمت الشبكات والاحتياجات التشغيلية لتحديد واستهداف المقاتلين الفرديين داخل هذه الشبكات، في هذا المعنى، فإنّ الحرب الإلكترونية تمثِّل شيئًا فريدًا حقًّا حول الطابع المتغير للحرب الحديثة، وتحديدًا ظاهرة المقاتلين الفرديين، ويدعى أن تصبح أهدافًا مشروعة لدولة الحرب والتركيز على الاستهداف التشغيلي.

ويبقى السؤال الأكبر حول ما إذا كان يمثِّل هذا النموذج التشغيلي تحولًا جوهريًّا ودائمًا في كيفية تنظيم أمريكا، تجهيز أجور مِثل هذه الصراعات في المستقبل، بالتناوب، فشنُّ هذه الحرب قد يمثِّل مجرد تحوُّل عابر من التركيز التقليدي على مؤسسة الأمن القومي إلى التقليدي، والحرب على غرار مناورة ضد الخصوم على أساس الدولة، والجواب على هذا السؤال ينطوي على قضية أكبر تعود إلى نموذج الحرب

حيث، مرة أخرى، يكون المقاتلون هم العامل المجهول في ساحة المعركة، المستهدفين على أساس الوضع بدلًا من الهُوية، عند هذه النقطة، فإنَّ الجواب على هذا السؤال ليس واضحًا تمامًا.



مستقبل الحرب الإلكترونية كسياسات واستراتيجيات: التحذير والاعتبارات

في الأسابيع التي عقبت هجمات 11/9، كانت الولايات المتحدة غير مستعدة إلى أي نزاع كان إلى حد كبير، وكان الجيش قد أنفق عقودًا من الحرب الباردة في تطوير النظريات والتقنيات الموجَّهة لاحتمال اشتباك القوة التقليدية ضد الخصوم على أساس الدولة، وغموض البيئة الأمنية خلال عام 1990 لم يَقُمْ بتغيير الكثير من قوة الجمود أو تحويل مؤسسة الأمن القومي من هذا التركيز الاستراتيجي الضيق نسبيًّا.

ومع ذلك، أدَّى الارتفاع التَّخريبي، والجهات الفاعلة التي لا تنتمي إلى دول مثل: تنظيم القاعدة وتجربة حملة مكافحة التمرد، التي طال أمدها حول التحول الجوهري في الكيفية التي يُنظر بها صناع قرار الأمن القومي إلى التهديدات الرئيسة لمصالح الولايات المتحدة، وردًّا على هذه التهديدات الجديدة التي تشمل التحولات الهيكلية والتقنية والوظيفية الأساسية، التي يضطلع بها في خضمِّ الصراع، نتيجة لذلك، وضعتِ الولايات المتحدة في نهاية المطاف قدرة فعَّالة بلا رحمة على مستوى العمليات لتحديد واستهداف الخلايا الصغيرة والمقاتلين الفرديين عبر ساحة المعركة، وكان لديها القدر نفسه من النجاح في تطبيق هذه التقنيات نحو مكافحة الإرهاب التي تركِّز على استهداف مجال أوسعَ مِن المساحات والمواقع التي لا تُسيطر عليها الحكومة؛ حيث كانت قوات الأمن المحلية إمَّا غير قادرة أو غير راغبة في إشراك هذه التهديدات.

على الجبهة الداخلية، استدانت الولايات المتحدة تقنيات مشابهة وأدوات إدارة المعلومات لدعم الاستراتيجيات القائمة على فَرْز الهوية؛ التي أَبقتِ الحدود وشبكات النقل، والمواطنين الأمريكيين آمنةً بشكل ملحوظ منذ 11/9، مع ذلك، في الوقت نفسه، كان الشيء المرجو من هذه الإنجازات التكتيكية والفنية البارزة التي لم يتم تسليمها بالكامل هو نهاية الدول السياسية على المستوى الاستراتيجي، هذا صحيح بشكل خاصٍّ فيما يتعلَّق باستقرار المناطق المضطربة، ووقف التجديد الدائم للتهديدات الفردية الناشئة من أماكن؛ مثل: أفغانستان والعراق واليمن والصومال وسوريا، وليبيا.

يمكن القول بأنَّ هذه الانتكاسات غيَّرت مجرى الحساب الاستراتيجي الأميركي، ربما لأجيال؛ كما تؤكد استراتيجية الأمن القومي للرئيس، تحول أمريكا بعيدًا عن الاستراتيجية التي تعتمد على القتال المكلف، الحروب البرية واسعة النطاق بدلًا من:

النهج الأكثر استدامة الذي يعطي الأولوية للعمليات التي تستهدف مكافحة الإرهاب، والعمل الجماعي مع الشركاء المسؤولين، وزيادة الجهود لمنع نموِّ التطرف العنيف والتطرف الذي يدفع إلى زيادة التهديدات. ولكن حتى مع هذه الكلمات من ضَبْط النفس، أكد الرئيس أن:

خارج مناطق القتال الفعلية، نحن نسعى لاحتجاز واستجواب الإرهابيين من خلال تطبيق القانون ومحاكمة المرتكبين، مع ذلك، عندما يكون هناك استمرار التهديد الوشيك، وعند يكون أسر الإجراءات لعرقلة التهديد أمرًا غير ممكن، فإنّنا لن نتردد في اتخاذ الإجراءات الحاسمة قولًا وعملًا، واقترحت الإدارة الحالية أنَّ العديد من الركائز الأساسية لنموذج الحرب الإلكترونية سوف تستمرُّ في لعب جزء من نهج استراتيجية الولايات المتحدة.

ومع ذلك، هذا يشير أيضًا إلى استراتيجية الأمن القومي التي سوف تركِّز في المقام الأول على التخفيف من حدة المخاطر بدلًا مِن الانتصار العسكري، قد تكون هذه الاستراتيجية لا تُقدِّم أي نهاية سياسية للدولة بشكل واضح بخلاف الهدف التكتيكي الفوري لتحديد وتحييد التهديدات الأكثر إلحاحًا لمصالح الولايات المتحدة الرئيسة والمواطنين، إذا كان هذا هو الحال، فإنَّ هذا سيكون شنًّا للصراع في المقام الأول مع المعلومات بدلًا من الأسلحة التقليدية، مع التركيز على الأدوات التقنية والمهارات المعرفية الأكثر قوة من النيران والمناورة.

وهذا النمط من الحرب سيستمر لسلالة حدود بيروقراطية تقليدية وفصل وظيفي بين سلطات إنفاذ القانون والإجراءات العسكرية، وأنشطة المخابرات، كما لاحظ أحد المعلقين في الآونة الأخيرة، أن طبيعة هذه التهديدات الأمنية الحديثة "تجعل من المستحيل تقريبًا رسم خطوط واضحة بين الحرب والسلام الأجنبية والمحلية، في حالات الطوارئ والحياة الطبيعية"، وهذا النمط من الحرب يصبح تطبيعًا، ومن المرجَّح أن يحدَّ أيضًا من قواعد الخصوصية المقبولة، وربما تَرَك آثارًا كبيرة على القضية الأكبر للهوية ومدى ارتباطها بالأمن القومي.

الخاتمة

في ختام هذه الدراسة، نُقدِّم عددًا قليلًا من التحذيرات والتوصيات:

أولا: يجب أن يوضع في الاعتبار أن الحرب الإلكترونية قد تطوَّرت في المقام الأول باعتبارها استراتيجية التكتيكات؛ أنها تمثل الأساليب والأدوات المصممة لعلاج الأعراض ولكن ليس المرض. الابتكارات العقائدية والتقنية للحرب الإلكترونية تتعامل مع التحديات التي تواجه عمليات محددة جدًّا من تحديد وفحص واستهداف الخصوم على أساس الشبكة والمقاتلين الفرديين، مع ذلك، فإنّها لا تملك إلا القليل جدًّا لتقدمه؛ من حيث التعامل مع الأسباب الكامنة وراء عدم الاستقرار والعنف السياسي.

لهذا السبب، يجب أن تُطبَّق أساليب الحرب الإلكترونية بحذر وبطريقة لا تَختلِط بين الاستهداف والاستراتيجية، وقد حذَّر الجنرال ماكماستر من "المداهمة العقلية" ومُغالَطة أنَّ الانتصارات الاستراتيجية يمكنها تحقيق ذلك ببساطة عن طريق تحديد عقد الشبكة الحيوية، ثم القضاء عليها من خلال الدقة، هناك قلق ذات صِلة، كما أنه يدل على زيادة براعة الولايات المتحدة في هذه الأساليب، وإنه سوف ينتج الثقة المفرطة في تقنيات الحرب الإلكترونية، وينبع هذا الحذر من الميل الأمريكي المتَّسِق للغاية مع الحلول التقنية العلمية لكل مشكلة أمنية وطنية، حتى عندما يفشل مرارًا وتكرارًا للوفاء بوعده الأول، وقد أثبت عقد من هذه الأساليب بوضوح مكانًا هامًّا للتكنولوجيات التي تقوم "بإزالة الدفاع عن عدم الكشف عن هوية المتطرف العنيف،" ومع ذلك، يجب ألا تكون فائدة هذه الأدوات في ذُروتها.

بغض النظر عن الخيارات الاستراتيجية المستقبلية، أسفرت الابتكارات الناجمة لشن الحرب الإلكترونية عن قدرات خارقة على الصعيدين التشغيلي والتكتيكي، هذه المهارات والأدوات والأساليب يجب أن

تستمرَّ إلى أن تنضج حتى تهدأَ المتطلبات التشغيلية المستمرة، ويشمل هذا مذهبي التقنية والابتكارات التنظيمية، والسياسة المحورية في شنِّ هذا النمط من الحرب. وتدل جميع المؤشرات على استمرار الأشكال المختلفة من الحرب الهجينة والتهديدات غير النظامية في المستقبل القريب، وسوف ينطوي هذا حتمًا على الأنشطة العسكرية الأمريكية في مناطق غير محكومة، مع أنظمة الهوية الضعيفة والخصوم العازمة على استخدام عدم الكشف عن الهوية للميزة التشغيلية؛ ولذلك تظهر الحاجة إلى التحقق من الهوية في ساحة المعركة، وعلى الحدود.

من حيث مذهب الابتكار، هناك خطر كبير من ركود الجيش على وجه الخصوص، كما تنجذب القوات العسكرية إلى الوراء في اتجاه التركيز التقليدي على انخراط القوة التقليدية ضد الخصوم على أساس الحرب الإلكترونية التي شُنَّتْ على مدى العقد الماضي، لا يمكن أن تتم المحاربة من الهواء وسوف تظل تعتمد على القوات البرية لجمع المعلومات الاستخباراتية المفيدة وأداء الاستهداف الفعال؛ لهذا السبب، يجب على المذاهب الناشئة من مخابرات الهوية وعمليات الهوية أن تستمرَّ حتى تنضج وتكون متكاملة في المفهوم المرن للعمليات العسكرية الكاملة.

ستتمُّ التحديات التقنية الرئيسة في اكتشاف واستغلال مجموعة من التوقيعات غير قياسية ومصادر البيانات (الإنترنت، وسائل الإعلام الاجتماعية، القياسات الحيوية، والطب الشرعي)، ودمج تلك المصادر مع تيارات الجمع التقليدية لتحسين الوعي الظرفي؛ وهذا يتطلَّب استمرار التحسن في مجالات مثل مواجهة الجمع البيومتري وتدخُّل الطب الشرعي السريع، فضلًا عن التقدم في تكامُل البيانات وتبادل المعلومات بين الدفاع، والاستخبارات، والأمن الداخلي، وهذه تتطلَّب أساليبَ جديدةً لمعالجة البيانات والأدوات التحليلية المصممة للتعامل مع كميات كبيرة من المعلومات حول التحديات الهائلة، التي تمثل تقنية غير منظمة لا يمكن أن تَنتظِر للأزمة المقبلة.

ومن حيث التغيير التنظيمي، فقد حان الوقت للاعتراف بأن التهديدات الحالية والمستقبلية سوف تستمرُّ في تقويض التمييز بين الدفاع الخارجي والأمن الداخلي، قد يكون فرد من الذين تم مواجهتهم في منطقة القتال له صلة أيضًا بموظف الجمارك في مطار "جون كينيدي" بنيويورك، وهو ضابط شرطة يقوم بإجراء عملية التوقيف الروتينية في "توكسون، أريزونا"، أو محلل مكافحة الإرهاب في وكالة الاستخبارات المركزية، أو المصالح البيروقراطية وحواجز التقنية، ويجب ألا يُمْنَع تبادل المعلومات القوية بين هذه الكيانات، هذا الإدراك يجب أن يصل إلى أكثر عملية متعمدة لإعادة تكوين جهاز الأمن الوطني مع الاندماج باعتباره المبدأ التنظيمي الأساسي، ومع ذلك، يجب أن تتضمَّن هذه المناقشة أيضًا إعادة تقييم الأطر القانونية والسياسية لضمان الحماية المناسبة للمعلومات، وكذلك الشيكات اللازمة للسلطة من أجل معالجة شواغل الحرية والخصوصية المدنية.

في البداية، أشار هذا التحليل كيفية تحدى نموذج الحرب الإلكترونية للجوانب الأساسية لبناء ستفاليا، بما في ذلك العديد من الأسس القانونية التي عرفتها سير الحرب في العصر الحديث، على مدى العقد الماضي، قد أثبتت الولايات المتحدة الكفاءة التكتيكية الرائعة في شنٍّ هذا النوع من الحرب، لا سيما التحديد والفرز، واستهداف المقاتلين الفرديين في جميع أنحاء العالم؛ ومع ذلك، فإنّ المناقشات المستمرة حول التخلص من المعتقلين في "غوانتانامو، كوبا"، الحدة على نطاق وتطبيق AUMF، والمخاوف العالقة على غير أرض المعركة القاتلة، التي تستهدف الجميع تشير إلى أن العديد من القضايا المتعلقة بسير الحرب الإلكترونية تبقى دون حل، إذا لم يكن هناك جدل.

إذا واصلت الولايات المتحدة العمل في إطار فرضية أن التهديدات، التي يُشكِّلها المقاتلون الفرديون تمثِّل الآن مصدرَ قلق للأمن القومي الكبير؛ بالتالي، فهي تهدُف إلى مشروع الحرب، وبذلك يجب أن يكون هناك إطار قانوني وأخلاقي وإرشادي حول: كيف يمكن لهذا النوع من شن الحرب أن يتم؟ من أجل أن يكون فعَّالًا، يجب أن يكون لهذا البناء نِطاقًا يُعادل السلطة على الهياكل القائمة، التي حددت شروط وحدود الصراع التقليدي على مدى عقود، وفيما يخصُّ أمريكا، فإنَّ هذا قد يعتبر حاجة بارزة بشكل خاص. باعتبارها القوة العظمى المتبقية في العالم، يجب أن يكون أمنها مستمدًّا شرعيًّا بشكل لا جدال فيه في استخدام القوة العسكرية ولا يهم اختيار الاستراتيجية، والأدوات، أو الأساليب.



المصادر

1. Sun Tzu, The Art of War, Thomas Cleary, trans., Boston, MA: Shambhala Pocket Classics, 1991.

2. Micah Zenko, “The U.S. Just Launched Its 500th Drone Strike,” Defense One, November, 21, 2014, available from www.defenseone.com/threats/2014/11/us-just-launched-its-500th-drone-129

strike/99722/?oref=defenseone_today_nl. Also, the New American Foundation, Long War Journal, and Bureau of Investigative Jour¬nalism all monitor U.S. drone strikes taking place outside the “ac¬tive combat zones” of Iraq, Afghanistan, and Libya. The 500 to¬tal strikes in Pakistan, Yemen, and Somalia represent an average among the range of estimates from these organizations as of No¬vember 2014. This number includes a total of seven U.S. citizens killed by drone strikes during the Obama administration.

3. Jo Becker and Scott Shane, “Secret ‘Kill List’ Proves a Test of Obama’s Principles and Will,” The New York Times, May 29, 2012.

4. Linda Robinson, Paul D. Miller, John Gordon IV, Jeffrey Decker, Michael Schwille, and Raphael S. Cohen, Improving Stra¬tegic Competence: Lessons from 13 Years of War, Santa Monica, CA: RAND, 2014, p. 26.

5. John Arquilla and David Ronfeldt, Networks and Netwars: The Future of Terror, Crime, and Militancy, Santa Monica, CA: RAND, 2001.

6. Thomas L. Friedman, The Lexus and the Olive Tree, New York: Anchor Books, 2000.

7. Arquilla and Ronfeldt.

8. Defense Science Board Task Force on Defense Intelligence, Counterinsurgency: Intelligence, Surveillance, and Reconnaissance Op¬erations,

Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2011, p. 52.

9. Martin van Creveld, The Rise and Decline of the State, New York: Cambridge University Press, 1999, pp. 162-163.

10. Jean-Jacques Rousseau, “The Social Contract,” Victor Gourevitch, ed., The Social Contract and Other Writings, New York: Cambridge University Press, 1997, p. 51.

11. Gabriella Blum, “The Individualization of War: From War to Policing in the Regulation of Armed Conflicts,” Austin Sarat, Lawrence Douglas, and Martha Merrill Umphrey, eds., Law and War: An Introduction, Redwood City, CA: Stanford University Press, 2014, p. 52.130

12. For elaboration on this concept, see Gabriella Blum, “The Dispensable Lives of Soldiers,” Journal of Legal Analysis, Vol. 2, No. 1, Spring 2010, pp. 115-147.

13. 10 U.S.C. § 948a: US Code, Section 948A defines “unprivi¬leged enemy belligerent” as an individual (other than a privileged belligerent) who (A) has engaged in hostilities against the United States or its coalition partners; (B) has purposefully and materi¬ally supported hostilities against the United States or its coalition partners; or (C) was a part of al Qaeda at the time of the alleged offense under this chapter.

14. Samuel Issacharoff and Richard Pildes, “Targeted War¬fare: Individuating Enemy Responsibility,” New York University Law Review, Vol. 88, No. 5, November 2013, p. 1,521.

15. In addition to dozens of journal articles on this topic, see “Forensics and Warrant Based Targeting,” March 2010, Ft. Leavenworth, KS: Center for Army Lessons Learned (CALL), for a detailed discussion of how this concept has been applied operationally.

16. van Creveld, p. 163.

17. There are certainly exceptions to this rule in American history, notably targeting against such figures as Poncho Villa, Hitler, Yamamoto, Gadhafi, Noriega, Mohammed Aideed, and Osama Bin Laden. However, as a practical matter prior to 9/11, leadership targeting was generally applied as a discrete military objective that was adjunct to the larger political purpose of the conflict. As such, it has not been a central feature of warfight¬ing strategies or formalized as part of doctrinal approaches until recently.

18. Benjamin Rhodes, Deputy National Security Advisor, from an interview with NPR. Quote reprinted in Bill Chappell, "U.S. Won't Rule Out Attack In Syria To Hit Islamic State," August 21, 2014, available from www.npr.org/blogs/thetwo-way/2014/08/21/342165273/u-s-won-t-rule-out-attack-in-syria-to-hit-islamic-state.131

19. Rosa Brooks, "There's No Such Thing as Peacetime," Foreign Policy, March 13, 2015, available from www.foreignpolicy.com/2015/03/13/theres-no-such-thing-as-peacetime-forever-war-terror-civil-liberties/.

20. John Abizaid and Rosa Brooks, Recommendations and Re¬port of the Task Force on US Drone Policy, Washington, DC: Stimson Center, June 2014, p. 12.

21. Among others, see recent discussions on this topic by Issacharoff and Pildes, and Gabriella Blum.

22. U.S. Joint Chief of Staff, Joint and Coalition Operational Analysis Division (J7), Decade of War Volume 1: Enduring Lessons from the Past Decade of Operations, Washington, DC: U.S. Joint Chiefs of Staff, June 15, 2012, p. 2.

23. U.S. Department of the Army, Field Manual (FM) 3-60, The Targeting Process, Washington, DC: Headquarters, Department of the Army, November 26, 2010, p. B-1.

24. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Report of the Defense Science Board Task Force on Defense Biometrics, Washington, DC: Defense Science Board, March 2007.

25. General David Petraeus, Commander, U.S. Central Command, Multi-National Force-Iraq, “Counterinsurgency Guidance,” June 21, 2008.

26. Targeting doctrine defines “high-value individuals,” or HVIs, as “persons of interest (friendly, adversary, or enemy) who must be identified, surveilled, tracked, and influenced through the use of information or fires.” See FM 3-60, p. B-1.

27. Christopher J. Lamb and Evan Munsing, Secret Weapon: High-Value Target Teams as an Organizational Innovation, Washing¬ton, DC: National Defense University Press, March 2011, p. 33.

28. Stanley McChrystal, “It Takes a Network: The New Front Line of Modern Warfare,” Foreign Policy, February 21, 2011, avail¬able from www.foreignpolicy.com/2011/02/21/it-takes-a-network/.132

29. Carlotta Gall, “Night Raids Curbing Taliban, but Afghans Cite Civilian Toll,” The New York Times, July 8, 2011. Also see Tom Peter, “Afghanistan: NATO’s Night Raids Cause More Harm than Good, Report Says,” The Christian Science Monitor, September 19, 2011.

30. Charles Faint and Michael Harris, “F3EAD: Ops/Intel Fusion Feeds The SOF Targeting Process,” Small Wars Journal, January 31, 2012.

31. U.S. Joint Forces Command, Commander’s Handbook for Attack the Network, Suffolk, VA: Joint Warfighting Center, Joint Doctrine Support Division, May 20, 2011.

32. Steve Ressler, “Social Network Analysis as an Approach to Combat Terrorism: Past, Present and Future Research,” Home¬land Security Affairs, Vol. 2, No. 2, July 2006.

33. See Duncan Watts, Six Degrees: The Science of a Connected Age, New York: W. W. Norton, 2003; and Small Worlds: The Dy¬namics of Networks between Order and Randomness, Princeton, NJ: Princeton University Press, 1999.

34. Ajay Mehra, Daniel Brass, Giuseppe Labianca, and Ste¬phen Borgatti, “Network Analysis in the Social Sciences,” Science, Vol. 323, No. 5916, February 13, 2009, pp. 892-895.

35. FM 3-24, Counterinsurgency, Washington, DC: Headquar¬ters, Department of the Army, December 15, 2006, Appendix B.

36. John A. Nagl, “The Evolution and Importance of Army/Marine Corps Field Manual 3-24, Counterinsurgency,” Foreword to the U.S. Army/Marine Corps Counterinsurgency Field Manual by the United States Army and United States Marine Corps, Chi¬cago, IL: University of Chicago Press, 2007, available from www.press.uchicago.edu/Misc/Chicago/841519foreword.html.

37. For useful analysis on the integration of SNA into the Ar¬my’s counterinsurgency doctrine, see David Knoke, “It Takes a Network: The Rise and Fall of Social Network Analysis in U.S. Army Counterinsurgency Doctrine,” and John A. Nagl, “Con¬structing the Legacy of Field Manual 3-24,” Joint Forces Quarterly, Vol. 58, pp. 118-120.133

38. FM 3-24, Appendix B.

39. FM 3-60, p. B-1.

40. Bob Woodward, “Why Did Violence Plummet? It Wasn’t Just the Surge,” The Washington Post, September 8, 2008, available from www.washingtonpost.com/wp-dyn/content/article/2008/09/07/AR2008090701847.html.

41. Joint Publication (JP) 3-24, Counterinsurgency, Washington, DC: U.S. Joint Chiefs of Staff, November 2013, p. XVI.

42. Joint Center for Operational Analysis, Operation IRAQI FREEDOM, January 2007 to December 2008 The Comprehensive Approach: An Iraq Case Study, Norfolk, VA: U.S. Joint Forces Command, February 2010, p. 14.

43. See Army Electronic Publication (ATP) 2-33.4 Intelligence Analysis, August 2014, JP 2.01-3 Joint Intelligence Preparation of the Operational Environment, June 2009, and FM 3-60.

44. Some critics remain skeptical with regard as to how fully the military has embraced these ideas and whether they still influ¬ence thinking about future warfighting concepts, particularly as many leaders advocate a return to

conventional warfighting ap¬proaches and doctrines. See Knoke for this contrasting viewpoint.

45. See United States Marine Corps (USMC) IdOps Strat¬egy 2020 and U.S. Department of the Navy, Marine Corps Order 5530.17, Marine Corps Identity Operations (IdOps), November 13, 2012.

46. Ibid.

47. Anthony Smith and Mark Schaefer, “More Than Just Bio¬metrics: Why Marine Corps Identity Operations are Critical to MAGTF Mission Success,” Marine Corps Gazette, Vol. 98, No. 5, May 2014.

48. Identity intelligence (I2) appeared for the first time as part of recognized doctrine in October 2013 in the updated version of JP 2.0, Joint Intelligence, then more recently in the latest version of 134

JP 3-05, Special Operations, July 2014, where it described I2 as “the collection, analysis, exploitation, and management of identity attributes and associated technologies and processes.”

49. JP 3-26, Counterterrorism, Washington, DC: U.S. Joint Chiefs of Staff, October 24, 2014, p. V-5.

50. Robert O. Work and Shawn Brimley, 20YY: Preparing for War in the Robotic Age, Washington, DC: Center for a New American Security, 2014, p. 17.

51. Antoine Bousquet, “Cyberneticizing the American War Machine: Science and Computers in the Cold War,” Cold War History, Vol. 8, No. 1, 2008.

52. Emily Mushen and Jonathan Schroden, Are we Winning? A brief History of Military Operations Assessment, Washington, DC: CNA Center for Stability and Development, 2014.

53. Charles Shrader, History of Operations Research in the U.S. Army, Volume III, 1973-1995, Washington, DC: Office of the Dep¬uty Under Secretary of the Army for Operations Research, 2009.

54. William Westmoreland, “Address to the Association of the U.S. Army,” October 14, 1969, cited in Antoine Bousquet, Cy¬bernetic Warfare: Computers and the Cold War, Meeting of Interna¬tional Studies Association, San Diego, CA, March 22, 2006.

55. Robert Tomes, “The Cold War Offset Strategy: Assault Breaker and the Beginning of the RSTA Revolution,” War on the Rocks Blog, November 20, 2014, available from www.warontherocks.com/2014/11/the-cold-war-offset-strategy-assault-breaker-and-the-beginning-of-the-rsta-revolution/.

56. Mark Mazzetti, The Way of the Knife, New York: Penguin Books, 2014, pp. 94-101. Also see Andrew Callam, “Drone Wars: Armed Unmanned Aerial Vehicles,” International Affairs Review, Vol. XVIII, No. 3, Winter 2010.

57. Jeremiah Gertler, U.S. Unmanned Aerial Systems, Washing¬ton, DC: Congressional Research Service, January 3, 2012.135

58. Amitai Etzioni, “The Great Drone Debate,” Military Review, Vol. 93, No. 2, March-April 2013, p. 2.

59. Andrew Callam, “Drone Wars: Armed Unmanned Aerial Vehicles,” International Affairs Review, Vol. XVIII, No. 3, Winter 2010.

60. Abizaid and Brooks, p. 11. Unclassified reporting suggests a significant increase in the use of such strikes during the Obama administration with 33 strikes in 2008 and 54 in 2009, killing at least 20 militant leaders. See Simon Frankel Pratt, “Crossing off Names: The Logic of Military Assassination,” Small Wars and Insurgencies, Vol. 26, No. 1, pp. 3-24.

61. Pratt.

62. Bill Roggio, “U.S. Military Confirms it Killed Islamic State, Shabaab Leaders in Airstrikes,” Long War Journal Blog, February 11, 2015, available from www.longwarjournal.org/archives/2015/02/us_military_confirms.php#ixzz3RWChIqrJ.

63. Micah Zenko, Reforming U.S. Drone Strike Policies, Wash¬ington, DC: Council on Foreign Relations, January 2013, p. 8.

64. U.S. Department of Defense, Defense Science Board Task Force on COIN and ISR Operations, Washington, DC: Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, February 2011, p. 65.

65. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, "Report of the Defense Science Board Task Force on Defense Biometrics," Washington, DC: Defense Science Board, March 2007, p. 39.

66. Anthony Iasso, "A Critical Time for Biometrics and Iden¬tity Intelligence," Military Intelligence Professional Bulletin, July-September 2013, pp. 39-40.

67. Timothy S. McWilliams and Nicholas J. Schlosser, "U.S. Marines in Battle: Fallujah," November-December 2004, Quan¬tico, VA: U.S. Marine Corps, 2014, p. 62. Also see Thom Shanker, "To Track Militants, U.S. Has System That Never Forgets a Face," 136

The New York Times, July 13, 2011, available from www.nytimes.com/2011/07/14/world/asia/14identity.html?_r=0.

68. Jody Kieffer and Kevin Trissell, "DOD Biometrics: Lifting the Veil of Insurgent Identity," Army AT&L Magazine, April-June 2010, pp. 14-17, available from
asc.army.mil/docs/pubs/alt/2010/2_AprMayJun/articles/14_DOD_Biometrics--Lifting_the_Veil_of_Insurgent_Identity_201002.pdf.

69. Myra Gray, "Defending the U.S. with Biometrics," Info-security, Vol. 6, No. 6, September/October 2009, pp. 24–25.

70. Spencer Ackerman, "U.S. Holds on to Biometric Database of 3 Million Iraqis," Wired Magazine, Danger Room Blog, December 21, 2011, available from www.wired.com/2011/12/iraq-biometrics-database/.

71. Additional Training for Leaders and More Timely Transmission of Data Could Enhance the Use of Biometrics in Afghanistan, Washing¬ton, DC: U.S. Government Accountability Office, April 2012, p. 1.

72. David Pendall and Cal Sieg, "Biometric-Enabled Intelli¬gence in Regional Command–East," Joint Forces Quarterly, Vol. 72, No. 1, January 2014, p. 70.

73. U.S. Army, Commander’s Guide to Biometrics in Afghanistan: Observations, Insights, and Lessons, Ft. Leavenworth, KS: Center for Army Lessons Learned, April 2011. Also see Additional Training for Leaders and More Timely Transmission of Data Could Enhance the Use of Biometrics in Afghanistan, p. 8.

74. “Biometrics in Afghanistan: The Eyes Have It,” The Econo¬mist, July 7, 2012, available from www.economist.com/node/21558263.

75. For a useful overview discussion of the issues and sum¬mary of various recidivism rate estimates, see Jennifer Elsea and Michael John Garcia, “Wartime Detention Provisions in Recent Defense Authorization Legislation,” Washington, DC: Congres¬sional Research Service, January 23, 2015, pp. 14-16.

76. Martin Chulov, “ISIS: The Inside Story,” The Guardian, De¬cember 11, 2014, available from www.theguardian.com/world/2014/dec/11/-sp-isis-the-inside-story.137

77. David Axe, “CSI Somalia: Interpol Targets Pirates,” Wired Magazine, Danger Room Blog, June 18, 2009, available from www.wired.com/2009/06/csi-somalia-interpol-targets-pirates/.

78. Antonia Greene, “Including Biometrics in Deployment Training Helps Soldiers Identify the Enemy,” U.S. Army Office of Public Affairs, 174th Infantry Brigade, April 30, 2012, avail¬able from www.army.mil/article/78894/Including_biometrics_in_deployment_training_helps_Soldiers_identify_the_enemy.

79. Deputy Secretary of Defense, Authority to Collect, Store, and Share Biometric Information of Non-U.S. Persons with U.S. Govern¬ment (USG) Entities and Partner Nations, Memorandum, Washing¬ton, DC, January 12, 2012.

80. VIBES, Leidos Product Publication, available from www.leidos.com/products/software/vibes.

81. Erik Bowman, “Game Changers in DoD Biometrics,” conference presentation at the 2012 Biometric Consortium, Sep¬tember 20, 2012, Tampa, FL,

available from www.biometrics.org/bc2012/presentations/Workshops/SS_Thur_900-1000a_Game%20Changers_Bowman.pdf.

82. U.S. Marine Corps, Marine Corps Forensic Enterprise Strate¬gy, April 20, 2010, p. 3, available from www.mccdc.marines.mil/Portals/172/Docs/SWCIWID/SWAAB/IW%20Reader/MCFES_Final%20%2020%20April.pdf.

83. Additional Planning and Oversight Needed to Establish an Enduring Expeditionary Forensic Capability, Washington, DC: U.S. Government Accountability Office, June 2013, p. 4.

84. Oliver Herion, “Expeditionary Forensic Support to Joint Force Commanders: What Changes or Considerations are War¬ranted?” Quantico, VA: U.S. Marine Corps Command and Staff College, April 2012, p. v.

85. Douglas Shontz, DNA as Part of Identity Management for the Department of Defense, Santa Monica, CA: RAND, 2010, p. 7.138

86. Michael Johnston, “Expeditionary Forensics: The War¬rior’s Science Revealing the Hidden Enemy,” Military Police, Spring 2009, pp. 5-7.

87. “U.S. Used Lab in Afghanistan to Confirm bin Laden’s DNA,” Associated Press, August 30, 2013, available from www.spokesman.com/stories/2013/aug/30/in-brief-us-used-lab-in-afghani¬stan-to-confirm.

88. Patrick Tucker, “Special Operators are Using Rapid DNA Readers,” Defense One, May 21, 2015, available from www.defenseone.com/technology/2015/05/special-operators-are-using-rapid-dna-readers/113383/?oref=defenseone_today_nl.

89. Marine Corps Forensic Enterprise Strategy, p. 5.

90. Additional Planning and Oversight Needed to Establish an En¬during Expeditionary Forensic Capability, p. 1.

91. Joop Voetelink, "EvBO: Evidence-Based Operations, How to Remove the Bad Guys from the Battlefield," Journal of Interna¬tional Law of Peace and Armed Conflict, Vol. 4, 2013, p. 195.

92. Thomas B. Smith and Marc Tranchemontagne, "Under¬standing the Enemy: The Enduring Value of Technical and Fo¬rensic Exploitation," Joint Forces Quarterly, Vol. 75, No. 4, October 2014, p. 124.

93. Anthony Iasso, "A Critical Time for Biometrics and Iden¬tity Intelligence," Military Intelligence Professional Bulletin, July-September 2013, pp. 39-40.

94. United States Government Accountability Office, "De¬fense Forensics: Additional Planning and Oversight Needed to Establish an Enduring Expeditionary Forensic Capability," June 2013, available from www.gao.gov/assets/660/655546.pdf.

95. Sandra I. Erwin, "As Defense, Intelligence Agencies Drown in Data, Technology Comes to the Rescue," Nation Defense Magazine, November 2014.

96. Stephen Mayhew, "U.S. Defense Department Biometrics Database Upgraded," DoD Press Release, as reported in Biometrics 139

Update, December 16, 2014, available from www.biometricupdate.com/201412/u-s-defense-department-biometrics-database-upgraded and www.dote.osd.mil/pub/reports/FY2013/pdf/army/2013dodabis.pdf.

97. Patrick Tucker, "Jihadi John and the Future of the Biomet¬rics Terror Hunt," Defense One, February 27, 2015, available from www.defenseone.com/technology/2015/02/jihadi-john-and-future-biometrics-terror-hunt/106263/?oref=defenseone_today_nl.

98. Siobhan Gorman, "How Team of Geeks Cracked Spy Trade," The Wall Street Journal, September 4, 2009, available from www.wsj.com/articles/SB125200842406984303.

99. Andy Greenberg and Ryan Mac, "How A 'Deviant' Phi¬losopher Built Palantir, A CIA-Funded Data-Mining Juggernaut," Forbes, August 14, 2013, available from www.forbes.com/sites/andygreenberg/2013/08/14/agent-of-

intelligence-how-a-deviant-philosopher-built-palantir-a-cia-funded-data-mining-juggernaut/.

100. George I. Seffers, “Army’s Talking Technology,” Sig¬nal Magazine, September 2011, available from www.afcea.org/content/?q=armys-talking-technology.

101. Erik Bowman, “Game Changers in DoD Biometrics,” and “Biometric Data Storage and Biometric Intelligence,” presenta¬tions at the 2013 Biometrics Big Data Symposium For Defense, Intelligence, Homeland Security and Law Enforcement, June 18, 2013, Washington, DC, p. 11, available from www.semanticom¬munity.info/@api/deki/files/27723/Bowman-TTC_Biometric_BigData_Conf_fl13.pdf.

102. For a useful recent overview, see Lisa Seghetti, “Visa Waiver Program,” William L. Painter, ed., Selected Issues in Homeland Security Policy for the 114th Congress, Washington, DC: Congressional Research Service, May 2015, pp. 38-41.

103. Alison Siskin, Visa Waiver Program, Washington, DC: Congressional Research Service, February 2014, pp. 5-8.

104. “FBI Announces Biometrics Suite’s Full Operational Ca¬pability,” FBI Press Release, September 23, 2014, available from www.fbi.gov/news/stories/2014/september/fbi-announces-biometrics-140

suites-full-operational-capability/fbi-announces-biometrics-suites-full-operational-capability.

105. Aliya Sternstein, “Homeland Security To Roll Out Bio¬metrics Along the Border This Summer,” Defense One, January 28, 2015, available from www.defenseone.com/technology/2015/01/homeland-security-roll-out-biometrics-along-bordersummer/103968/?oref=defenseone_today_nl. Also see “OBIM Wants Info on Biometric Matching Systems,” PlanetBiometrics, April 28, 2015, available from www.planetbiometrics.com/article-details/i/2981/desc/obim-wants-info-on-biometric-matching-systems/, accessed April 29, 2015. See more at

www.planetbiometrics.com/article-details/i/2981/desc/obim-wants-info-on-biometric-matching-systems/#sthash.qFSOtHkQ.dpuf.

106. Amanda Vicinanzo, “Vulnerabilities in Coast Guard’s Biometric System May Impede Identification of Suspected Ter¬rorists,” Homeland Security Today, March 14, 2015, available from www.hstoday.us/briefings/daily-news-analysis/single-article/vulnera¬bilities-in-coast-guards-biometric-system-may-impede-identification-of-suspected-terrorists/bc0e386816bcc3e25b64ebcbd7ee3309.html.

107. Stephen Mayhew, “Obama’s New National Security Strategy Makes a Push for Biometrics Data Sharing,” Biometric Update, February 10, 2015, available from www.biometricupdate.com/201502/obamas-new-national-security-strategy-makes-a-push-for-biometrics-data-sharing.

108. This information includes, but is not limited to, biomet¬ric data: finger scans and digital facial photographs; encounter data: place and date of visa issuance; and biographic data: name, date of birth, gender, physical details, and visa issuance or visa refusal data.

109. The Consular Consolidated Database (CCD). For a com¬plete discussion, see Ruth Ellen Wasem, Immigration: Visa Security Policies, Washington, DC: Congressional Research Service, June 2014, p. 6.

110. Wasem.

111. Kathleen Kiernan, ‘‘Counterintelligence and Law En¬forcement,’’ Jennifer Sims and Burton Gerber, eds., Vaults, Mirrors 141

& Masks: Rediscovering U.S. Counterintelligence, Washington, DC: Georgetown University Press, 2009, p. 159.

112. John Wagner, Written testimony of CBP Office of Field Operations Acting Deputy Assistant Commissioner John Wagner for a House Committee on Oversight and Government Reform, Subcommittee on National Security hearing titled “Border Secu¬rity Oversight, Part III: Border Crossing Cards and B1/B2 Visas,” November 14, 2013, available from

www.dhs.gov/news/2013/11/14/written-testimony-cbp-house-oversight-and-government-reform-sub¬committee-national.

113. Currently, citizens of 38 countries may travel to the Unit¬ed States without a visa as part of the Visa Waiver Program based on the 2007 Homeland Security Presidential Directive 6 legislation. For a useful discussion, see a recent post on the Lawfare blog by Nathan Sales, “Is the Visa Waiver Program a Threat to our Na¬tional Security?” February 2, 2015, available from www.lawfare¬blog.com/2015/02/is-the-visa-waiver-program-a-threat-to-our-national-security/.

114. Martin Rudner, “Intelligence-Led Air Transport Security: Pre-Screening for Watch-Lists, No-Fly Lists to Forestall Terrorist Threats,” International Journal of Intelligence and Counterintelligence, Vol. 28, No. 1, 2015, p. 48.

115. National Counterterrorism Center, Terrorist Identities Datamart Environment (TIDE) Factsheet, August 2014, available from www.nctc.gov/docs/tidefactsheet_aug12014.pdf.

116. Adam Goldman, “More than 1 Million People are List¬ed in U.S. Terrorism Database,” The Washington Post, August 5, 2014, available from www.washingtonpost.com/world/national-security/more-than-1-million-people-are-listed-in-us-terrorism-data¬base/2014/08/05/a66de30c-1ccc-11e4-ab7b-696c295ddfd1_story.html.

117. Ibid.

118. Ken Kroupa, “An Inside Look at DoD’s DNA,” presen¬tation delivered at the 2010 Biometrics Consortium, September 21-23, 2010, Tampa, FL, available from www.biometrics.org/bc2010/presentations/RapidDNA/kroupa-An-Inside-Look-at-DoD-s-DNA.pdf.142

119. “Report of the Defense Science Board Task Force on Defense Biometrics,” p. 31.

120. FBI CODIS: National DNA Index (NDIS), FBI Homep¬age, available from www.fbi.gov/about-us/lab/biometric-analysis/codis/ndis-statistics.

121. Gefrides and Welch.

122. Patrick Tucker, “Special Operators are Using Rapid DNA Readers,” Defense One, May 21, 2015, available from www.defenseone.com/technology/2015/05/special-operators-are-using-rapid-dna-readers/113383/?oref=defenseone_today_nl.

123. Thomas B. Smith and Marc Tranchemontagne, “Un¬derstanding the Enemy: The Enduring Value of Technical and Forensic Exploitation,” Joint Forces Quarterly, Vol. 75, Fall 2014, pp. 122-128.

124. “Next Generation Identification, FBI Announces Bio¬metrics Suite’s Full Operational Capability,” FBI Press Release, September 23, 2014, available from www.fbi.gov/news/stories/2014/september/fbi-announces-biometrics-suites-full-operational-capability/fbi-announces-biometrics-suites-full-operational-capability.

125. Robert Schroeder, “A Strategic Evolution: A Path to Bor¬der Security,” Holding the Line in the 21st Century, Washington, DC: U.S. Customs and Border Protection, p. 38.

126. Justin Lee, “Customs’ Facial Recognition Technology Trial Raises Privacy Concerns,” Biometric Update, May 29, 2015, available from www.biometricupdate.com/201505/customs-facial-rec¬ognition-technology-trial-raises-privacy-concerns.

127. Authorization for the Use of Military Force (AUMF), Joint Resolution 23, 107th Cong., 1st sess., September 14, 2001. Also see Public Law § 2(a), 115 Stat, p. 224.

128. John O. Brennan, “The Efficacy and Ethics of U.S. Coun¬terterrorism Strategy,” public remarks delivered at the Wilson Center, April 30, 2012, available from www.wilsoncenter.org/event/the-efficacy-and-ethics-us-counterterrorism-strategy.143

129. John Yoo, “Assassinations or Targeted Killings since 9/11,” New York Law School Review, Vol. 57, 2011, p. 63.

130. According to recent polling, while Americans gener¬ally are concerned over government surveillance, some 82 per¬cent say it is acceptable to monitor communications of suspected terrorists. For details of recent polling, see Lee Rainie and Mary Maddens, "Americans' Privacy Strategies Post-Snowden," Pew Research Center, March 16, 2015, available from www.pewinter-net.org/2015/03/16/americans-privacy-strategies-post-snowden/. For public opinion on drone strikes, see Sarah Kreps, "Do Americans Really Love Drone Strikes?" The Washington Post, June 6, 2014.

131. George W. Bush, Homeland Security Presidential Directive (HSPD-6, Directive on Integration and Use of Screening Information To Protect Against Terrorism), September 16, 2003, available from www.gpo.gov/fdsys/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1174.pdf.

132. George W. Bush, Directive on Biometrics for Identification and Screening to Enhance National Security, June 5, 2008, available from www.gpo.gov/fdsys/pkg/PPP-2008-book1/pdf/PPP-2008-book1-doc-pg757.pdf. Also see DoD Instruction on Defense Biometric and Forensic Enabled Intelligence (DoD O-3300.bb), directing DoD to make available to other U.S. Government agencies, to the full¬est extent permitted by law, all biometric and associated infor¬mation on persons posing a threat to national security. Biometric data collected by DoD is integrated into the Automated Biometric Identification System (ABIS) and shared with the Department of Homeland Security, FBI, and various elements of the intelligence community.

133. Dennis C. Blair, Senate Select Committee on Intelligence, U.S. Intelligence Community Annual Threat Assessment 2010, Febru¬ary 3, 2010, available from www.dni.gov/files/documents/Newsroom/Testimonies/20100203_testimony.pdf.

134. Steve Coll, "The Unblinking Stare: The Drone War in Pakistan," The New Yorker, November 24, 2014.

135. One recent notable example was the January 2015 drone strike that accidentally killed two hostages held by al-Qaeda, one 144

of them an American. Similar strikes also killed two Americans who were reportedly members of al-Qaeda, Ahmed Farouq and Adam Gadahn, who were not specifically targeted as part of the operation. See Peter Baker and Julie Hirschfeld Davis, “2 Qaeda Hostages Were Accidentally Killed in U.S. Strike, White House Says,” The New York Times, April 23, 2015, available from www.nytimes.com/2015/04/24/world/asia/2-qaeda-hostages-were-acciden¬tally-killed-in-us-raid-white-house-says.html?hp&action=click&pgtype=Homepage&module=span-ab-top-region&region=top-news&WT.nav=top-news.

136. Patrick Tucker, “How Special Operators Are Taking Artificial Intelligence To War,” Defense One, May 28, 2015, avail¬able from www.defenseone.com/technology/2015/05/how-special-oper¬ators-are-taking-artificial-intelligence-war/113872/?oref=defenseone_today_nl.

137. Danya Greenfield, “The Case Against Drone Strikes on People Who Only ‘Act’ Like Terrorists,” The Atlantic, August 19, 2013. Also see Civilian Casualties & Collateral Damage at the Brook¬ings Institute Lawfare Blog, available from www.lawfareblog.com/wiki/the-lawfare-wiki-document-library/targeted-killing/controversy.

138. Greg Miller, “Plan for Hunting Terrorists Signals U.S. Intends to Keep Adding Names to Kill Lists,” Washington Post, October 23, 2012.

139. Comment by Micah Zenko, a scholar at the Council on Foreign Relations and the lead author of a 2013 study of drone warfare. See Scott Shane, “Drone Strikes Reveal Uncomfortable Truth: U.S. is Often Unsure About Who Will Die,” The New York Times, April 23, 2015, available from www.nyti.ms/1JiGHtY.

140. See Brennan, “The Efficacy and Ethics of U.S. Counter¬terrorism Strategy.” Also, one recent example of this policy was the capture of a “top al-Qaeda operative” and American citizen, Muhanad Mahmoud al Farekh, in Pakistan, who was reportedly nominated to the Pentagon’s “kill list” of suspected terrorists in 2013; however, he was captured by Pakistani forces and secret¬ly flown to the United States to face federal terrorism charges. See Adam Goldman and Tim Craig, “American Citizen Linked to al-Qaeda is Captured, Flown Secretly

to U.S.," The Washing¬ton Post, April 2, 2015, available from www.washingtonpost.com/145

world/national-security/american-citizen-suspected-of-being-al-qae¬da-member-captured-brought-to-us/2015/04/02/48e8cc4c-d89c-11e4-8103-fa84725dbf9d_story.html.

141. Christopher Lamb and Evan Munsing, Secret Weapon: High-Value Target Teams as an Organizational Innovation, Washing¬ton, DC: Institute for National Strategic Studies, National Defense University, 2011, p. 53.

142. Tom Peter, "In Iraq, Troops Balance Fighting and Lend¬ing a Hand," The Christian Science Monitor, August 7, 2008, avail¬able from www.csmonitor.com/World/Middle-East/2008/0807/p06s01-wome.html.

143. Gabriella Blum, "The Individualization of War: From War to Policing in the Regulation of Armed Conflicts," Sarat, Douglas, and Umphrey, eds., Law and War, Stanford, CA: Stanford Univer¬sity Press, 2013, available from www.ssrn.com/abstract=2231168.

144. For a useful discussion of World War II as a "scientists' war," see Paul Kennedy, Engineers of Victory: The Problem Solvers who Turned the Tide in the Second World War, New York: Random House, 2013.

145. See articles on personality identification playing cards, available from www.defenselink.mil/news/Apr2003/pipc10042003.html; and Tom Zucco, "Troops Dealt an Old Tool," St. Petersburg Times, April 12, 2003, available from www.sptimes.com/2003/04/12/Worldandnation/Troops_dealt_an_old_t.shtml.

146. Sydney J. Freedberg, "Raiders, Advisors and the Wrong Lessons from Iraq," Breaking Defense, March 20, 2013, available from www.breakingdefense.com/2013/03/gen-mcmaster-raiders-advisors-and-the-wrong-lessons-from-iraq.

147. Barrack Obama, "Remarks by the President at the Na¬tional Defense University, Speech at the National Defense Uni¬versity, May 23, 2013, transcript

available from www.whitehouse.gov/the-press-office/2013/05/23/remarks-president-national-defense-university.146

148. Adam Grissom, “The Future of Military Innovation Studies,” The Journal of Strategic Studies, Vol. 29, No. 5, October 2006, p. 907.

149. For one perspective on this distinction, see Stephen Rosen, Winning the Next War: Innovation and the Modern Military, Ithica, NY: Cornell University Press, 1991.

150. President Barack Obama, Interview on Fareed Zakaria GPS, February 1, 2015, transcript available from transcripts.cnn.com/TRANSCRIPTS/1502/01/fzgps.01.html.

151. Patrick Tucker, “What Happens When Spies Can Eaves¬drop on Any Conversation?” Defense One, December 1, 2014, available from www.defenseone.com/technology/2014/12/what-happens-when-spies-can-eavesdrop-any-conversation/100142/?oref=defenseone_today_nl.

152. Jim Garamone, “Capabilities Must Match Future Threats, Army Leader Says,” DoD News, Defense Media Activity, Febru¬ary 24, 2015, available from www.defense.gov/news/newsarticle.aspx?id=128237.

153. U.S. National Intelligence Council, Global Trends 2030: Al¬ternative Worlds, Washington, DC: U.S. Director of National Intel¬ligence, December 2012, pp. 59–60.

154. Matthew G. Olsen, Director of the National Coun¬terterrorism Center, Hearing before the Senate Committee on Homeland Security, “Worldwide Threats to the Homeland,” September 17, 2014, available from www.nctc.gov/docs/2014_world¬wide_threats_to_the_homeland.pdf.

155. Howard Altman, “Experience Briefing President Leads New Agency Chief to Raise Bar,” The Tampa Tribune, November 14, 2014, available from www.tbo.com/list/military-news/experience-briefing-president-leads-new-agency-chief-to-raise-bar-20141114.

156. Global Trends 2030, p. 50.

157. Ken Dilanian, “20,000 Foreign Fighters Flock to Syria, Iraq,” Associated Press, February 10, 2015, available from news.147

yahoo.com/ap-exclusive-20-000-foreign-fighters-flock-syria-211811073.html.

158. Eric Schmitt and Michael Schmidt, “West Struggles to Halt Flow of Citizens to War Zones,” The New York Times, January 13, 2015, available from www.nytimes.com/2015/01/13/world/west-struggles-against-flow-to-war-zones.html.

159. “Report on Foreign Terrorist Fighters,” New York: United Nations, March 2015, pp. 14-23.

160. Ibid., pp. 18-23.

161. Greg Miller, “Backlash in Berlin Over NSA Spying Re¬cedes as Threat from Islamic State Rises,” The Washington Post, December 29, 2014, available from www.washingtonpost.com/world/national-security/backlash-in-berlin-over-nsa-recedes-as-islamic-state-rises/2014/12/29/c738af28-8aad-11e4-a085-34e9b9f09a58_story.html.

162. Ahmed Rashid, “Waking Up to the New al-Qaeda,” New York Review of Books, January 12, 2015, available from www.ny-books.com/blogs/nyrblog/2015/jan/12/paris-attacks-waking-al-qaeda.

163. John Mueller and Mark Stewart, “How French Intel¬ligence Missed the Charlie Hebdo Terrorists,” Time, January 14, 2015, available from www.time.com/author/john-mueller-and-mark-stewart.

164. Alissa J. Rubin, “Lawmakers in France Move to Vastly Expand Surveillance,” The New York Times, May 5, 2015, available from www.nytimes.com/2015/05/06/world/europe/french-legislators-approve-sweeping-intelligence-bill.html?_r=0.

165. An expression coined by NATO officials and first used during the 2014 Crimean crisis, referring to masked Russian sol¬diers and military equipment within Ukraine.

166. Assessment by the International Institute for Strategic Studies (IISS) in the annual Military Balance report, see Radio Free Europe/Radio Liberty, “Report Warns Russia’s Hybrid Warfare In Ukraine Could Inspire Others,” February 11, 2015, available from www.rferl.org/content/russia-hybrid-warfare-ukraine-could-in¬spire-others/26842566.html.148

167. Agence France-Press, “French Soldiers In Mali Stalked By Invisible Enemy,” May 30, 2015, available from www.defnews.ly/1HCvUFn.

168. Patrick Tucker, “What Happens When Spies Can Eaves¬drop on Any Conversation?” Defense One, December 1, 2014, avail¬able from www.defenseone.com/technology/2014/12/what-happens-when-spies-can-eavesdrop-any-conversation/100142/.

169. Elizabeth Young, “Summary of the “Decade of War,” Prism, Vol. 4, No. 2, 2013, p. 126.

170. Alan Gelb and Julia Clark, “Identification for Develop¬ment: The Biometrics Revolution,” Washington, DC: Center for Global Development, January 2013, p. 7.

171. “UN begins biometric registration of Rwandans in DRC,” Planet Biometrics, April 13, 2015, available from www.planetbiomet¬rics.com/article-details/i/2905/.

172. Justin Lee, “UNHCR, Accenture Provide Global Bio¬metric Identity Management System to Help Refugees,” Biomet¬ric Update, May 25, 2015, available from www.biometricupdate.com/201505/unhcr-accenture-provide-global-biometric-identity-man¬agement-system-to-help-refugees.

173. Jennifer Hicks, “United Nations High Commissioner For Refugees Adopts Biometric Tracking,” Forbes, May 31, 2015, avail¬able from www.forbes.com/sites/jenniferhicks/2015/05/30/united-nations-high-commissioner-for-refugees-adopts-biometric-tracking/.

174. Rosa Brooks, “Know Thy Enemy, and the Future of Memorial Day,” Foreign Policy, May 25, 2015, available from

www.foreignpolicy.com/2015/05/25/drones-dna-facebook-future-war-memorial-day/.

175. Charles J. Dunlap, Jr., “The Hyper-Personalization of War: Cyber, Big Data, and the Changing Face of Conflict,” George¬town Journal of International Affairs, Vol. 15, 2014, pp. 108-118.

176. Estimate based on a recent technology market research report by ABI Research. See Anna Forrester, “Commercial Seg¬ment to Overtake Government in Biometrics Spending by 2017,” 149

ExecutiveBiz Blog, February 11, 2015, available from www.blog.ex-ecutivebiz.com/2015/02/abi-research-commercial-segment-to-overtake-govt-in-biometrics-spending-by-2017/.

177. Justin Lee, “U.S. Government Biometrics Spend to Reach US$8.6 B by 2020: ABI Research,” Biometrics Update, April 20, 2015, available from www.biometricupdate.com/201504/u-s-government-biometrics-spend-to-reach-us8-6-b-by-2020-abi-research.

178. Zack Martin, “Goode Predicts Mobile Biometric Growth,” Secure ID News, February 4, 2014, available from www.secure¬idnews.com/news-item/goode-predicts-mobile-biometric-growth/#. Ar¬ticle references the monthly industry report by Goode Intelligence entitled, “Fingerprint Biometrics and Mobile and Wearable Bio¬metrics.”

179. Gelb and Clark.

180. “Government and technology: Playing leapfrog: The Wonders of Smart Systems,” The Economist, May 24, 2015, avail¬able from www.economist.com/node/21651330/print.

181. UK Home Office, Guidance Notes, “Biometric Residence Permits, General Information for Applicants, Employers and Sponsors,” March 2015, available from www.gov.uk/government/uploads/system/uploads/attachment_data/file/413959/v_4_BRP_-_Ge¬neric_information_leaflet_2_March_-_6_April__clean_.pdf.

182. “Nigerian Communications Commission Deploys BIO-Key Fingerprint Technology for National SIM Card Registration Program,” Marketwired, May 28, 2013, available from www.fi¬nance.yahoo.com/news/nigerian-communications-commission-deploys-bio-120000546.html.

183. Tim Craig and Shaiq Hussain, “Pakistanis Face a Deadline: Surrender Fingerprints or Give up Cellphone,” The Washington Post, February 23, 2015, available from www.washingtonpost.com/world/asia_pacific/pakistanis-face-a-deadline-surren¬der-fingerprints-or-give-up-cellphone/2015/02/23/de995a88-b932-11e4-bc30-a4e75503948a_story.html?utm_source=Sailthru&utm_medium=email&utm_term=%2ASituation%20Report&utm_campaign=Sit%20Rep%20February%2025%202015.150

184. Paul Roderick Gregory, “Putin’s New Weapon In The Ukraine Propaganda War: Internet Trolls,” Forbes, December 9, 2014, available from www.forbes.com/sites/paulroderickgrego¬ry/2014/12/09/putins-new-weapon-in-the-ukraine-propaganda-war-internet-trolls/.

185. Department of Defense Cyber Strategy, Washington, DC: U.S. Government Printing Office, April 2015, p. 12.

186. Linda Kinstler, “Global Cyber Defense Demand Will Exceed Capability for Years To Come,” Defense One, January 28, 2015, available from www.defenseone.com/technology/2015/01/global-cyber-defense-demand-will-exceed-capability-years-come/103983/.

187. Chris White, “New Search Engine Exposes the Dark Web,” Interview with CBS 60 Minutes with the DARPA devel¬oper on a new technology for searching internet “dark web” sites, February 8, 2015, available from www.cbsnews.com/news/new-search-engine-exposes-the-dark-web.

188. Tor, or The Onion Routing project, was originally devel¬oped by the U.S. Naval Research Laboratory for the purpose of protecting government communications and is now used by a wide variety of private and commercial interests. For a discussion of the potential for anonymous use of Bitcoin, see Craig Elwell, Maureen Murphy, and Michael Seitzinger, Bitcoin: Questions, An-swers,

and Analysis of Legal Issues, Washington, DC: Congressional Research Service, January 28, 2015, p. 3.

189. Mark Wallace, Written Testimony before the House Com¬mittee on Foreign Affairs Subcommittee on Terrorism, Nonprolif¬eration, and Trade, "The Evolution of Terrorist Propaganda: The Paris Attack and Social Media," January 27, 2015, available from www.counterextremism.com/press/counter-extremism-project-ceo-mark-wallace-testify-house-committee-foreign-affairs.

190. Tim Fernholz, "Terrorism Finance Trackers Worry ISIS Already Using Bitcoin," February 13, 2015, Defense One, available from www.defenseone.com/threats/2015/02/terrorism-finance-trackers-worry-isis-already-using-bitcoin/105345/?oref=defenseone_today_nl.151

191. Patrick Tucker, "How the Military Will Fight ISIS on the Dark Web," February 24, 2015, Defense One, available from www.defenseone.com/technology/2015/02/how-military-will-fight-isis-dark-web/105948/?oref=defenseone_today_nl.

192. National Intelligence Council, Global Trends 2030: Alter¬native Worlds, Washington, DC: National Intelligence Council, De¬cember 2012, p. 128, available from www.dni.gov/files/documents/GlobalTrends_2030.pdf.

193. Matthew G. Olsen, Hearing before the Senate Committee on Homeland Security, "Worldwide Threats to the Homeland," September 17, 2014.

194. Gabriel Weimann, New Terrorism and New Media, Wash¬ington, DC: Commons Lab of the Woodrow Wilson International Center for Scholars, 2014, p. 1.

195. Michael Chertoff and Tobby Simon, "The Impact of the Dark Web on Internet Governance and Cyber Security: Global Commission on Internet Governance Paper Series No. 6," Water¬loo, Ontario, Canada: Centre for International Governance Inno¬vation and the Royal Institute for International Affairs, February 2015, p. 1.

196. Patrick Tucker, “What Your Facebook Posts Mean to U.S. Special Operations Forces,” Defense One, January 29, 2015, avail¬able from www.defenseone.com/technology/2015/01/what-your-face¬book-posts-mean-usspecialforces/104031/?oref=defenseone_today_nl.

197. Marc Lynch, Deen Freelon, and Sean Aday, “Syria’s Socially Mediated Civil War,” Peaceworks, No. 91, January 2014, available from www.usip.org/sites/default/files/PW91-Syrias%20So-cially%20Mediated%20Civil%20War.pdf.

198. Weimann, p. 2; and Haroro Ingram, “Three Traits of the Islamic State’s Information Warfare,” The RUSI Journal, Vol. 159, No. 6, 2004, pp. 4-11.

199. J. M Berger and Jonathon Morgan, The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twit¬ter, Analysis Paper No. 20, Washington, DC: Brookings Project 152

on U.S. Relations with the Islamic World, March 2015, p. 2. Also see Brian Bennett, “With Islamic State Using Instant Messaging Apps, FBI Seeks Access to Data,” The Los Angeles Times, June 10, 2015, available from www.latimes.com/world/middleeast/la-fg-terror-messaging-20150608-story.html#page=1 1/5.

200. Joseph Carter, Shiraz Maher, and Peter Neumann, #Greenbirds: Measuring the Importance and Influence of Foreign Fighter Networks, London, UK: The International Centre for the Study of Radicalization and Political Violence, April 2014, avail¬able from www.icsr.info/wp-content/uploads/2014/04/ICSR- Report-Greenbirds-Measuring-Importance-and-Infleunce-in-Syrian-Foreign-Fighter-Networks.pdf.

201. Joe Parkinson and Maria Abi-Habib, “How Jihadists Slip Through Europe’s Dragnet and Into Syria,” The Wall Street Jour¬nal, February 20, 2015, available from www.wsj.com/articles/how-jihadists-slip-through-europes-dragnet-and-into-syria-1424653670.

202. Julian Barnes, “U.S. Military Plugs into Social Media for Intelligence Gathering,” The Wall Street Journal, August 6, 2014, available from

www.wsj.com/articles/u-s-military-plugs-into-social-media-for-intelligence-gathering-1407346557.

203. James Rupert, “Russian Troops Lead Moscow’s Biggest Direct Offensive in Ukraine Since August,” January 23, 2015, At¬lantic Council, available from www.atlanticcouncil.org/blogs/new-atlanticist/russian-special-forces-and-regular-troops-lead-moscow-s-biggest-direct-offensive-in-ukraine-since-august.

204. Daniel Regalado, Nart Villeneuve, and John Scott Rail¬ton, Behind the Syrian Conflict’s Digital Front Lines, Milpitas, CA: Firefly Inc., February 2015, p. 5.

205. Behind the Syrian Conflict’s Digital Front Lines, p. 18.

206. Brian Everstine, “Carlisle: Air Force Intel Uses ISIS ‘Mo¬ron’s’ Social Media Posts to Target Airstrikes,” Air Force Times, June 4, 2015, available from www.airforcetimes.com/story/military/tech/2015/06/04/air-force-isis-social-media-target/28473723/.

207. See “The ISIS Twitter Census,” as one recent example.153

208. “Anonymous ‘Hacktivists’ Strike a Blow against ISIS,” Anonymous website, available from www.anonhq.com/anonymous-hacktivists-strike-blow-isis.

209. David Sanger and Eric Schmitt, “Hackers Use Old Lure on Web to Help Syrian Government,” The New York Times, Febru¬ary 1, 2015, available from www.nytimes.com/2015/02/02/world/mid¬dleeast/hackers-use-old-web-lure-to-aid-assad.html?_r=0.

210. Generically, “OPSEC” refers to a process that identifies one’s own critical information and determines if it can be ob¬tained by adversaries and exploited for their use. It also includes the use of measures that eliminate or reduce these risks.

211. Johann Wolfgang von Goethe, Maxims and Reflections, Bailey Saunders, trans., New York: The MacMillan Company, 1906, available from onlinebooks.library.upenn.edu/webbin/gutbook/lookup?num=33670.

212. Charles J. Dunlap, Jr., “The Hyper-Personalization of War: Cyber, Big Data, and the Changing Face of Conflict,” Vol. 15, Georgetown Journal of International Affairs, 2014, p. 113.

213. Michael Shear and Scott Shane, “White House Weighs Sanctions after Second Breach of a Computer System,” The New York Times, June 12, 2015, available from www.nytimes.com/2015/06/13/us/white-house-weighs-sanctions-after-second-breach-of-a-computer-system.html?hp&action=click&pgtype=Homepage&module=first-column-region&_r=0.

214. Patrick Radden Keeke, “Rocket Man: How an Unem¬ployed Blogger Confirmed that Syria had Used Chemical Weap¬ons,” The New Yorker, November 25, 2013, available from www.newyorker.com/magazine/2013/11/25/rocket-man-2.

215. The same individual involved in the Syrian chemical weapons reporting also founded Bellingcat, a forum for citizen investigative journalism with a focus on military and security issues. See www.bellingcat.com.

216. Paul Rosenzweig, Cyberwarfare: How Conflicts in Cy¬berspace are Challenging America and Changing the World, Santa Barbara, CA: ABC-CLIO, 2013, p. 20.154

217. Weimann, p. 10.

218. Patrick Tucker, “What Happens When You Pose as the Defense Secretary on Twitter?” Defense One, December 2, 2014, available from www.defenseone.com/technology/2014/12/what-happens-when-you-pose-next-defense-secretary-twitter/100304/.

219. Bruce Schneier, “Hacker or Spy? In Today’s Cyberat¬tacks, Finding the Culprit is a Troubling Puzzle,” The Christian Science Monitor, March 4, 2015, available from www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0304/Hacker-or-spy-In-today-s-cyberattacks-finding-the-culprit-is-a-troubling-puzzle.

220. Greg Miller, “CIA Looks to Expand its Cyber Espio¬nage Capabilities,” The Washington Post, February 23, 2015, available from www.washingtonpost.com/world/national-security/cia-looks-to-expand-its-cyber-espionage-capabilities/2015/02/23/a028e80c-b94d-11e4-9423-f3d0a1ec335c_story.html?utm_source=Sailthru&utm_medium=email&utm_term=%2ASituation%20Report&utm_campaign=Sit%20Rep%20February%2025%202015.

221. Carl von Clausewitz, On War, Michael Howard and Peter Paret, eds. and trans., Princeton, NJ: Princeton University Press, 1976, p. 595.

222. For doctrinal discussion on this issue, see JP 5-0, Joint Operation Planning, Chap. III, “Operational Art and Operational Design,” August 11, 2011.

223. Mary Madden and Lee Rainie, “Americans’ Attitudes about Privacy, Security, and Surveillance,” Pew Research Center, May 20, 2015, available from: www.pewinternet.org/2015 /05/20/americans-attitudes-about-privacy-security-and-surveillance/.

224. Ibid. Some 69 percent of adults say they are not confident that records of their activity maintained by the social media sites they use will remain private and secure, while only 9 percent say they feel they have “a lot” of control over how much information is collected about them and how it is used.

225. Sydney Freedberg, “6 Threats, 6 Changes, & A Brave New World: Intel Chief Vickers,” Breaking Defense, January 21, 2015, available from www.breakingdefense.com/2015/01/6-threats-6-changes-a-brave-new-world-intel-chief-vickers.155

226. Brian Barrett, “Can Google’s Future-Lab Finally Kill the Password?” Wired, May 29, 2015, available from www.wired.com/2015/05/google-atap-passwords-vault-io/.

227. Evelyn Brown, Performance of Facial Recognition Software Continues to Improve, Washington, DC: National Institute of Stan¬dards and Technology, June 3, 2014, available from www.nist.gov/itl/iad/face-060314.cfm. Data based on a

research study conducted by Patrick Grother and Mei Ngan, “Performance of Face identifi¬cation Algorithms.”

228. Andrea Peterson, “The Biometrics Revolution is Already Here—and You May Not be Ready For It,” The Washington Post, October 17, 2014, available from www.washingtonpost.com/blogs/the-switch/wp/2014/10/17/the-biometrics-revolution-is-already-here-and-you-may-not-be-ready-for-it.

229. Yaniv Taigman, Ming Yang, Marc’Aurelio Ranzato, and Lior Wolf, “DeepFace: Closing the Gap to Human-Level Performance in Face Verification,” Facebook Research Publication, Menlo Park, CA and Tel Aviv University, Tel Aviv, Israel, 2014, available from https://research.facebook.com/publications/480567225376225/deepface-closing-the-gap-to-hu¬man-level-performance-in-face-verification/. Also see Tom Si-monite, “Facebook Creates Software That Matches Faces Al¬most as Well as You Do,” MIT Technology Review, March 17, 2014, available from www.technologyreview.com/news/525586/facebook-creates-software-that-matches-faces-almost-as-well-as-you-do/, accessed January 7, 2015.

230. National Science and Technology Council (NSTC) Com¬mittee on Homeland and National Security, Subcommittee on Biometrics, Introduction to Biometrics, pp. 129-130, available from www.biometrics.gov/ReferenceRoom/Introduction.aspx.

231. Major distorting factors are referenced by the acronym, APIER—aging, pose, illumination, expression, and resolution.

232. Patrick Grother and Mei Ngan, “Face Recognition Ven¬dor Test: Performance of Face Identification Algorithms,” Wash¬ington, DC: Department of Commerce, National Institute of Stan¬dards and Technology, May 26, 2014, available from www.nist.gov/customcf/get_pdf.cfm?pub_id=915761.156

233. Stephan Mracek, Jan Vana, Radim Dvorak, and Svetlana Yanushkevich, “3D and Thermo-Face Fusion,” Jucheng Yang and Shan Juan Xie, eds., New Trends and Developments in Biometrics, Intech, November 28, 2012, available from www.intechopen.com/books/new-trends-and-developments-in-biometrics.

234. Erik Sofge, “The End of Anonymity,” Popular Science, January 15, 2014, available from www.popsci.com/article/technology/end-anonymity.

235. While not exclusively useful for identification purposes, physiological characteristics and thermal markers might be em¬ployed for screening individuals suspected of having certain medical issues, fever, etc.

236. Babak Hodjat, “Myth Busting Artificial Intelligence,” Wired Magazine, February 19, 2015, available from www.wired.com/insights/2015/02/myth-busting-artificial-intelligence/.

237 . Robert Hof, “Deep Learning,” MIT Technology Review, April 23, 2013, available from www.technologyreview.com/featured¬story/513696/deep-learning.

238 . Quentin Hardy, “Facebook Offers Artificial Intelligence Tech to Open Source Group,” January 16, 2015, The New York Times, available from bits.blogs.nytimes.com/2015/01/16/facebook-offers-artificial-intelligence-tech-to-open-source-group/.

239. Jose Pagliery, “FBI Launches a Face Recognition Sys¬tem,” CNN.com, September 16, 2014, available from www.money.cnn.com/2014/09/16/technology/security/fbi-facial-recognition.

240. “The Face Detection Algorithm Set To Revolutionize Im¬age Search,” MIT Technology Review, February 16, 2015, referenc¬ing the paper by Sachin Sudhakar Farfade, Mohammad Saberian, and Li-Jia Li, “Multi-view Face Detection Using Deep Convolu¬tional Neural Networks,” February 10, 2015, available from www.arxiv.org/abs/1502.02766.

241. James Albers, “The Truth about Biometric Exit Tech¬nology,” Security Today, October 1, 2014, available from www.security-today.com/articles/2014/10/01/the-truth-about-biometric-exit.157

aspx. StereoVision recently demonstrated a Wireless 3D Binocular Face Recognition System in response to a Navy contract for tech¬nologies focused on “stand-off identification of uncooperative subjects.” See Patrick Tucker, “The

Navy's New Binoculars Can Identify You From 700 Feet Away," Defense One, May 15, 2015.

242. Alex Hern, "Hacker Fakes German Minister's Finger¬prints," The Guardian, December 30, 2014, available from www.the-guardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands.

243. Peter Counter, "New Iris Innovations May Bring Eye-Based Biometrics to the Masses," Mobile ID World, January 15, 2015, available from www. mobileidworld.com/new-iris-innovations-may-bring-eye-based-biometrics-to-the-masses-1151.

244. Sean Lyngaas, "Can the Pentagon Keep Pace on Bio¬metrics?" FCW.com, March 11, 2015, available from fcw.com/Articles/2015/03/11/Can-the-Pentagon-keep-pace-on-biometrics.aspx?m=2&p=1.

245. Ibid.

246. Federal Bureau of Investigation, "Image-Based Matching Technology Offers Identification and Intelligence Prospects," FBI Press Release, December 2012, available from https://www.fbi.gov/about-us/cjis/cjis-link/december-2012/Image-Based%20Matching%20Technology%20Offers%20Identification%20and%20Intelligence%20Prospects.

247. Douglas Reynolds, "Speaker Verification: From Research to Reality," Paper presented at the 2002 Institute of Electrical and Electronics Engineers (IEEE), International Conference Acoustics, Speech, and Signal Processing, May 13-17, 2002, available from www.ll.mit.edu/mission/cybersec/publications/publication-files/full_papers/020513_Reynolds.pdf.

248. Taylor Haney, The Future of Voiceprints, Los Angeles, CA: Annenberg Media Center, December 27, 2014, available from www.neontommy.com/news/2014/12/future-voiceprints.

249. Patrick Tucker, “What Happens When Spies Can Eaves¬drop on Any Conversation?” Defense One, December 1, 2014, 158

available from www.defenseone.com/technology/2014/12/what-hap¬pens-when-spies-can-eavesdrop-any-conversation/100142/.

250. Homayoon Beigi, “Speaker Recognition: Advancements and Challenges,” Jucheng Yang and Shan Juan Xie, eds., New Trends and Developments in Biometrics, Intech, November 28, 2012, available from www.intechopen.com/books/new-trends-and-develop¬ments-in-biometrics.

251. NSTC, Committee on Homeland and National Secu¬rity, Subcommittee on Biometrics, Introduction to Biometrics, pp. 129-130, available from www.biometrics.gov/ReferenceRoom/Introduction.aspx.

252. VIBES Product Information Sheet from the Leidos Corp-oration, Reston, VA, available from www.leidos.com/sites/default/files/files/14-0439vFc-VIBES_FS.pdf.

253. Rachel Metz, “Deep Learning Squeezed onto a Phone,” MIT Technology Review, February 9, 2015, available from www.technologyreview.com/news/534736/deep-learning-squeezed-onto-a-phone.

254. Ray Locker, “Military Could Be Using High-Tech Speech Software by 2017,” USA Today, February 22, 2015, available from www.usatoday.com/story/news/nation/militaryintelligence/2015/02/22/robust-speech-translation-transcription-soft¬ware/23839041/.

255. “Laboratory Team Takes Honors at the 2014 Audio/Vi¬sual Emotion Challenge and Workshop,” MIT Lincoln Laboratory, The Bulletin, January 9, 2015.

256. Chuck Brooks, “Human Factors and Biometrics at DHS,” Biometric Update, August 1, 2014, available from www.biometricup-date.com/201408/human-factors-and-biometrics-at-dhs.

257. DARPA, Detection & Computational Analysis ofPsychological Signals Information Sheet, May 2013, avail-able from www.

webcache.googleusercontent.com/search?q=cache:mM_FJrE2m7oJ:www.darpa.mil/opencatalog/DCAPShtml+&cd=2&hl=en&ct=clnk&gl=us.159

258. Norberto Andradejun, “Computers Are Getting Better Than Humans at Facial Recognition,” The Atlantic, June 9, 2014, available from www.theatlantic.com/technology/archive/2014/06/bad-news-computers-are-getting-better-than-we-are-at-facial-recognition/372377.

259. Roman Yampolskiy and Venu Govindaraju, “Behavioral Biometrics: A Survey and Classification,” International Journal of Biometrics, Vol. 1, No. 1, 2008, p. 81.

260. Ibid., p. 88.

261. Julian Barnes, “U.S. Military Plugs into Social Media for Intelligence Gathering, Defense Intelligence Agency Head Says Online Postings Played Crucial Role in Ukraine Jet Shootdown,” The Wall Street Journal, August 6, 2014, available from www.wsj.com/articles/u-s-military-plugs-into-social-media-for-intelligence-gath¬ering-1407346557.

262. Peter Counter, “Behavioral Biometrics to Become In¬creasingly Standard in Fraud Detection,” FindBiometrics, July 23, 2014, available from www.findbiometrics.com/behavioural-biometrics-to-become-increasingly-standard-in-fraud-detection.

263. Boer Deng, “People Identified through Credit-Card Use Alone,” Nature, January 29, 2015, available from www.nature.com/news/people-identified-through-credit-card-use-alone-1.16817.

264. For one recent example of these applications, see pat¬ent filing for Israeli behavioral biometrics firm BioCatch. Related article available from “BioCatch Granted Behavioural Biometric Patent for Mobiles,” Planet Biometrics, February 25, 2015, available from www.planetbiometrics.com/article-details/i/2746.

265. James Vincent, “Behaviosec uses Behavioral Biometrics to Find If the Person Using a Mobile Device Is Really Who They Claim to Be,” The Independent, September 2, 2014, available from

www.economictimes.indiatimes.com/news/international/business/behaviosec-uses-behavioural-biometrics-to-find-if-the-person-us¬ing-a-mobile-device-is-really-who-they-claim-to-be/articleshow/41463585.cms.160

266. Aliya Sternstein, “NSA Trying to Track Your Smart¬phone Finger Strokes,” Defense One, May 26, 2015, available from www.defenseone.com/technology/2015/05/nsa-trying-track-your-smartphone-finger-strokes/113638/??oref=d_brief_nl.

267. Yedid Hoshen and Shmuel Peleg, “Egocentric Video Bio¬metrics,” Jerusalem, Israel: The Hebrew University of Jerusalem, November 27, 2014, available from Cornell University Library at www.arxiv.org/pdf/1411.7591v1.pdf.

268. Rachel Metz, “Deep Learning Squeezed onto a Phone,” MIT Technology Review, February 9, 2015, available from www.technologyreview.com/news/534736/deep-learning-squeezed-onto-a-phone/.

269. Yampolskiy and Govindaraju, p. 93.

270. D. A. Reid, S. Samangooei, C. Chen, M. S. Nixon, and A. Ross, “Soft Biometrics for Surveillance: An Overview,” C. R. Rao and Venu Govindaraju, eds., Handbook of Statistics, Vol. 31, Oxford, UK: Elsevier, 2013.

271. Daniel Reid and Mark Nixon, “Imputing Human Descrip¬tions in Semantic Biometrics,” paper presented at the Multimedia in Forensics, Security and Intelligence conference, Florence, Italy, October 2010, available from eprints.soton.ac.uk/271623/1/mifor541-reid.pdf.

272. J. Thornton, J. Baran-Gale, D. Butler, M. Chan, and H. Zwahlen, “Person Attribute Search For Large-Area Video Sur¬veillance,” IEEE Conference on Technologies for Homeland Security, 2011, available from ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6107847&url=http%3A%2F%2Fieeexplore.ieee.org%2Fstamp%2Fstamp.jsp%3Ftp%3D%26arnumber%3D6107847.

273. The probability that two unrelated individuals would share all 13 pairs of alleles used in the FBI’s n 13 core short tan¬dem repeat (STR) profile is estimated

to be one in several hun¬dred billion. See Nathan James, "DNA Testing in Criminal Justice: Background, Current Law, Grants, and Issues," Washington, DC: Congressional Research Service, December 6, 2012, p. 3.161

274. Another method involves the use of mitochondrial DNA (mtDNA) sequencing that is useful for evidence samples such as hair fragments, bones, and teeth. This analysis is highly sensitive and therefore can be used in cases with limited biological material or degraded samples. However, because mtDNA profiles are only shared between maternal family members, this method is not as discriminating as STR analysis for identification.

275. Lisa Gefrides and Katie Welch, "Forensic Biology: Serol¬ogy and DNA," Ashraf Mozayani and Carla Noziglia, eds., The Forensic Laboratory Handbook Procedures and Practice, New York: Springer, 2011, p. 28.

276. DNA Casework Unit (DCU) Information Page, FBI web¬site, available from www.fbi.gov/about-us/lab/biometric-analysis/dna-casework-unit-dcu-1.

277. FBI Rapid DNA or Rapid DNA Analysis, FBI homepage, available from www.fbi.gov/about-us/lab/biometric-analysis/codis.

278. Kathy Pretz, "New System to Speed Up DNA Analy¬sis," The Institute, February 4, 2013, available from theinstitute.ieee.org/technology-focus/technology-topic/new-system-to-speed-up-dna-analysis. For a technical description, see Melissa May, "Field-De¬ployable Rapid DNA Analysis: Fully Integrated, Fully Automat¬ed Generation of Short Tandem Repeat Profiles of Buccal Swabs," IEEE Conference on Technologies for Homeland Security, 2011.

279. Patrick Tucker, "Special Operators are Using Rapid DNA Readers," Defense One, May 21, 2015, available from www.defenseone.com/technology/2015/05/special-operators-are-using-rapid-dna-readers/113383/?oref=defenseone_today_nl.

280. Gefrides and Welch, "Forensic Biology: Serology and DNA," p. 39.

281 . Isaacson et al., “Robust Detection of Individual Forensic Profiles in DNA Mixtures,” Forensic Science International: Genetics, Vol. 14, January 2015, pp. 31–37.

282. Eric Schwoebel, “Genomic Analysis and Human Iden¬tification,” briefing slides and discussions with author, Lexing¬ton, MA: MIT Lincoln Laboratory, January 9, 2013. Also, Melissa 162

Gymrek et al., “Indentifying Personal Genomes by Surname Infer¬ence,” Science, January 18, 2013, available from www.sciencemag.org/content/339/6117/321.full.

283. Douglas Shontz, DNA as Part of Identity Management for the Department of Defense, Santa Monica, CA: RAND, 2010, p. 9.

284. David Pendall, Global Operations and Biometrics: Next Gen¬eration Capabilities and Policy Implications, Carlisle, PA: U.S. Army War College, 2013, p. 4.

285. Andrew Pollack, “Building a Face, and a Case, on DNA,” The New York Times, February 23, 2015, available from www.nytimes.com/2015/02/24/science/building-face-and-a-case-on-dna.html?_r=0.

286. Pendall, p. 26.

287. Sandra I. Erwin, “As Defense, Intelligence Agencies Drown in Data, Technology Comes to the Rescue,” National Defense Magazine, November 2014, available from www.nationaldefensemagazine.org/archive/2014/November/Pages/AsDefenseIntelligenceAgenciesDrowninData,TechnologyComestotheRescue.aspx.

288. Aparna Garg and Allan Ramsay, “Semantic Content Analysis of Video: Issues and Trends,” W. Lin et al., eds., Mul¬timedia Analysis, Processing & Communications, Berlin, Germany: Springer-Verlag, 2011, pp. 443–457.

289. John, Markoff, “Researchers Announce Advance in Image-Recognition Software,” The New York Times, November, 17, 2014, available from

www.nytimes.com/2014/11/18/science/researchers-announce-breakthrough-in-content-recognition-software.html?_r=0.

290. Tom Simonite, “A Startup’s Neural Network Can Under¬stand Video,” MIT Technology Review, February 3, 2015, available from www.technologyreview.com/news/534631/a-startups-neural-net¬work-can-understand-video/.

291. For a discussion of this research, see Andrew Gallagher, Clint Mathialagan and Dhruv Batra, “VIP: Finding Important 163

People in Images,” February 9, 2015, available from www.arxiv.org/abs/1502.05678.

292. Tom Simonite, “Google’s Brain-Inspired Software De¬scribes What It Sees in Complex Images,” MIT Technology Review, November 18, 2014, available from www.technologyreview.com/news/532666/googles-brain-inspired-software-describes-what-it-sees-in-complex-images.

293. George Seffers, “Tag Teaming Big Data,” Big Data ebook, Fairfax, VA: AFCEA International, 2014, p. 13.

294. Conor Dougherty, “Google Translate App Gets an Up¬grade,” The New York Times, January 14, 2015, available from www.bits.blogs.nytimes.com/2015/01/14/google-translate-app-gets-an-upgrade/?hp&action=click&pgtype=Homepage&module=second-column-region&_r=0.

295 . Hardy, “Facebook Offers Artificial Intelligence Tech to Open Source Group.”

296. Davey Alba, “The Startup That Helps You Analyze Twit¬ter Chatter in Real Time,” Wired Magazine, February 12, 2015, available from www.wired.com/2015/02/luminoso/.

297. Ben Shneiderman, Carsten Gorg, Chaomei Chen, Jim Thomas, John Stasko, and Pak Chung Wong, “Graph Analytics—Lessons Learned and Challenges Ahead,” IEEE Computer Graphics and Applications, Vol. 33, No. 5,

September/October 2011, pp. 18-29, available from www.cs.umd.edu/~ben/papers/Wong2011Graph.pdf.

298. William Campbell, Charlie Dagli, and Clifford Weinstein, “Social Network Analysis with Content and Graphs,” Lincoln Lab¬oratory Journal, Vol. 20, No. 1, 2013, pp. 61-81, available from www.ll.mit.edu/publications/journal/pdf/vol20_no1/20_1_5_Campbell.pdf.

299 . David Stillwella, Michal Kosinskia, and Thore Graepel, “Private Traits and Attributes are Predictable from Digital Re¬cords of Human Behavior,” Proceedings of the National Acade¬my of Sciences, Early Edition, March 11, 2013, available from www.pnas.org/cgi/doi/10.1073/pnas.1218772110.164

300. For one such example, see Ana-Maria Popescu and Marco Pennacchiotti, “A Machine Learning Approach to Twitter User Classification,” Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media, Association for the Advancement of Artificial Intelligence, 2011, available from www.aaai.org/ocs/index.php/ICWSM/ICWSM11/paper/viewFile/2886/3262.

301. These traits represent the so-called “big five,” or the five-factor model of personality considered to be the most comprehen¬sive, reliable, and useful set of personality concepts. For discus¬sion of use of social media for personality analysis, see Daniele Quercia, David Stillwell, Jon Crowcroft, and Michal Kosinski, “Our Twitter Profiles, Our Selves: Predicting Personality with Twitter,” available from www.cl.cam.ac.uk/~dq209/publications/quercia11twitter.pdf.

302. Renaud Lambiotte and Michal Kosinski, “Tracking the Digital Footprints of Personality,” Proceedings of the IEEE, Vol. 102, No. 12, December 2014, pp. 1934-1939, available from ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6939627&url=http%3A%2F%2F ieeexplore.ieee.org%2Fxpls%2Ficp.jsp%3Farnumber%3D6939627.

303. Ibid.

304. Siobhan Peters and Craig Denholm, “Channel: Protecting Vulnerable People from Being Drawn into Terrorism: A Guide for Local Partnerships,” London, UK: Office for Security and Counter-Terrorism, Home Office, October

2012, available from www.gov.uk/government/uploads/system/uploads/attachment_data/file/118194/channel-guidance.pdf.

305. Mark Townsend, "How a Team of Social Media Experts Is Able to Keep Track of the UK Jihadis," The Guardian, January 17, 2015, available from www.theguardian.com/world/2015/jan/17/social-media-british-jihadists-islamic-state-facebook-twitter.

306. Katrin Bennhold, "Fertile Ground for Militancy in Home¬town of Jihadi John," The New York Times, February 28, 2015, avail¬able from www.nytimes.com/2015/03/01/world/europe/fertile-ground-for-militancy-in-hometown-of-jihadi-john.html?_r=0.165

307. Social Network Analysis with Content and Graphs, p. 73.

308. Jihun Hamm, Adam Champion, Guoxing Chen, Mikhail Belkin, and Dong Xuan, "Crowd-ML: A Privacy-Preserving Learning Framework for a Crowd of Smart Devices," Columbus, OH: The Ohio State University, Department of Computer Science and Engineering, January 11, 2015, available from www.arxiv.org/abs/1501.02484.

309. Social Network Analysis with Content and Graphs, p. 68.

310. Eric Schmitt, "U.S. Intensifies Effort to Blunt ISIS' Mes¬sage," The New York Times, February 16, 2015, available from www.nytimes.com/2015/02/17/world/middleeast/us-intensifies-effort-to-blunt-isis-message.html?_r=0.

311. Derek O'Callaghan, Derek Greene, Joe Carthy, Maura Conway, Nico Prucha, and Padraig Cunningham, "Online Social Media in the Syria Conflict: Encompassing the Extremes and the In-Betweens," research paper sponsored by the Cybercrime Cen¬ters of Excellence Network and Science Foundation Ireland (SFI), August 13, 2014, available from www.arxiv.org./abs/1401.7535.

312. See discussion of the computational science and informa¬tion science campaign plans in the Technical Implementation Plan: 2015-2019, Adelphi, MD:

U.S. Army Research Laboratory, Janu¬ary 2015, available from www.arl.army.mil/www/pages/172/docs/ARL_Technical_Implementation_Plan.pdf.

313. Elizabeth Dwoskin, “Sleuthing Search Engine: Even Bet¬ter Than Google?” The Wall Street Journal, February 12, 2015, avail¬able from www.wsj.com/articles/sleuthing-search-engine-even-better-than-google-1423703464.

314. Rita Boland, “Novel Big Data Reveals Global Human Behavior,” Big Data ebook, Fairfax, VA: AFCEA International, 2014, p. 13.

315. For background information, see the homepage for the Institute for the Study of Violent Groups, available from www.isvg.org/organization.php.166

316. Amelia Thomson-Deveaux, “Tracking 125,000 Incidents of Global Terrorism,” FiveThirtyEight, January 23, 2015, available from fivethirtyeight.com/features/the-paris-attacks-are-just-a-few-of-125000-entries-in-the-global-terrorism-database.

317. U.S. Army Training and Doctrine Command (TRA- DOC) Pamphlet (TP) 525-3-1, The U.S. Army Operating Concept: Win in a Complex World, Fort Eustis, VA: TRADOC, 2014, p. 33.

318. Barrack Obama, National Security Strategy of the United States, Washington, DC: The White House, February 2015.

319. Rosa Brooks, “There’s No Such Thing as Peacetime,” Foreign Policy, March 13, 2015.

320. Lieutenant General Michael Barbero, Testimony before the House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, Washington, DC, July 12, 2012.